ИСКУССТВО ОБМАНА

Кевин Д. Митник

Вильям Л. Саймон

Вильям Л. Саймон
Кевин Митник

Искусство обмана

Искусство обмана: Компания АйТи; 2004
ISBN 5-98453-011-2, 0-471-23712-4

Аннотация

Книга The Art of Deception – «Искусство обмана» – доказывает, насколько мы все уязвимы. В современном мире, где безопасность подчас выходит на первый план, на защиту компьютерных сетей и информации тратятся огромные деньги. Деньги тратятся на технологии безопасности. Эта книга объясняет, как просто бывает перехитрить всех защитников и обойти технологическую оборону, как работают социоинженеры и как отразить нападение с их стороны Кевин Митник и его соавтор, Бил Саймон рассказывают множество историй, которые раскрывают секреты социальной инженерии. Авторы дают практические советы по защите от атак, по обеспечению корпоративной безопасности и снижению информационной угрозы «Искусство обмана» не только демонстрирует, насколько опасна и вредоносна социоинженерия, но поможет разработать собственную программу тренинга по безопасности для сотрудников компании.

Содержание

Неопубликованная глава 7
Рассказ Кевина 8
Финальные выводы 29
Введение 31
Предисловие 33
С чего всё начиналось 34
От телефонного фрикинга к хакингу 36
Становление социальным инженером 39
Финальные выводы 42
Вступление 44
Глава 1: Самое слабое звено в безопасности 47
Человеческий фактор 48
Классический случай обмана 51
Характер угрозы 55
Злоупотребление доверием 59
Террористы и обман 63
Об этой книге 65
Глава 2: Когда безвредная информация опасна 69
Скрытая ценность информации 70
CREDITCHEX 71
Частный сыщик в действии 75
Западня для инженера 82

Ещё одна «ничего не стоящая» информация 90
Предотвращение обмана 93
Глава 3: Прямая атака: просто попроси 98
Случай с центром назначения линий 99
Юноша в бегах 101
На пороге 104
Заговаривание зубов (Отвлекающая болтовня) 107
Глава 4: Внушая доверие 114
Доверие: ключ к обману 115
Вариации по теме: Сбор кредитных карт 121
Одноцентовый сотовый телефон 127
Взлом федералов 131
Предотвращение обмана 136
Глава 5: «Разрешите Вам помочь» 139
Неполадки в сети 140
Немного помощи для новенькой девушки. 150
Не так безопасно, как думаешь 155
Предотвращение обмана 171
Глава 6: «Не могли бы Вы помочь?» 177
Чужак 178
Неосторожный руководитель 187
Глава 7: Фальшивые сайты и опасные приложения 204
«Не желаете ли вы бесплатно …?» 206
Сообщение от друга 212

Вариации по теме 214
Вариации по вариации 219
Глава 8: Используя чувство симпатии, вины и запугивание 228
Визит в студию 229
«Сделайте это сейчас» 233
«Мистер Бигг хочет это» 238
Что знает о вас администрация общественной безопасности 242
Один простой звонок 250
Полицейский набег 257
Переводя стрелки 264
Предупреждение обмана 270
Глава 9: Ответный удар 275
Исскуство дружелюбного убеждения 276
Глава 11: Сочетая технологию и социальную инженерию 301
Взлом решетки 302
Быстрое скачивание 314
Легкие деньги 317
Словарь как орудие атаки 326
Предотвращение обмана 337
Глава 13: Умные мошенники 343
Несоответствующий “Caller ID” 344
Вариация: Звонит президент Соединенных Штатов 350
Невидимый сотрудник 354

Полезный секретарь 358
Суд по делам дорожного движения 361
Возмездие Саманты 368
Предотвращение обмана 372
Глава 14: Промышленный шпионаж 376
Глава 15: Знание об информационной безопасности и тренировки 377
Обеспечение безопасности с помощью технологии, тренировки и процедуры 378
Понимание того, как атакующий может воспользоваться человеческой природой 380
Создание тренировочных и образовательных программ 386
Тестирование 398
Поддержание бдительности 399
«Зачем мне все это?» 402
Краткое описание безопасности в организации 403
Определение атаки 404
Проверка и классификация информации 408

Кевин Митник, Вильям Саймон Искусство обмана

Неопубликованная глава

Перевод: Yarlan Zey (yarlan@pisem.net)

(Это оригинальная глава, значительно сокращенная в опубликованной версии книги.)

Я неохотно писал этот раздел, потому что я был уверен, что он будет звучать эгоистично. Ну, хорошо, он эгоистичен. Но со мной связывались буквально сотни людей, которые хотели знать «кто такой Кевин Митник?». Если вам безразлично, обратитесь к Главе 2. Для всех остальных, кого это ещё волнует, вот мой рассказ.

Рассказ Кевина

Некоторые хакеры стирают чужие файлы или целые жёсткие диски; их называют кракерами или вандалами. Некоторые из хакеров-новичков не заботятся об изучении технологии, они просто скачивают хакерский инструмент для взлома компьютерных систем; их называют script kiddies. Более опытные хакеры с навыками в программировании разрабатывают хакерские программы и рассылают их по сети и ББСкам. И ещё, есть индивидуумы, которые не интересуются технологией, они просто используют компьютер для захвата чужих денег, товаров или услуг. Не смотря на миф о Кевине Митнике, созданный медиа, я не злонамеренный хакер. То, что я делал, даже не было противозаконно, когда я это начал, но стало преступлением после принятия нового законодательства. Я всё равно продолжал это делать и был пойман. Моя тяжба с правительством была основана не на преступлениях, а на создании из моего случая прецедента. Я не заслужил, чтобы меня преследовали как террориста или опасного преступника: обыскивали мою квартиру с неподписанным ордером; сажали в одиночную камеру на целые месяцы; отказывали в фундаментальных конституционных правах, гарантированных любому преступ-

нику; отказывали не только в залоге, но и в слушании залога; и годами бороться, чтобы получить правительственные улики, чтобы мои адвокаты смогли подготовиться к моей защите.

Что касается моего права на быстрое испытание? Каждые шесть месяцев втечение нескольких лет я стоял перед выбором: подписать бумагу об отказе от конституционного права на быстрое испытание или пройти через испытание с неподготовленным адвокатом; я выбирал первое. Но я отклоняюсь от своего рассказа. Возможно, мой жизненный путь сложился в ранней юности. Я был счастливым ребёнком, но маялся от скуки. После того как мой отец разбился, когда мне было 3, моя мать работала официанткой, чтобы нас прокормить. Она целыми днями работала по сумасшедшему графику и я почти всё время был предоставлен сам себе. Я сам был своей няней. Жизнь в долине Сан-Фернандо открыла мне возможность исследовать целый Лос-Анджелес, и к 12 годам я обнаружил, как можно бесплатно путешествовать по всей великой Л.А. долине. Однажды я обнаружил, что водители используют необычную модель дырокола, чтобы отмечать на билете день, время и маршрут. Отвечая на мои тщательно подготовленные вопросы, знакомый водитель рассказал мне, где можно купить такой дырокол. Обычно со своим билетом вы можете только пересесть на другой автобус и продолжить поездку в своём напра-

влении, но я разработал способ как бесплатно путешествовать в любом направлении. Чистые билеты можно было найти в парке: мусорные корзины около автобусных терминалов всегда переполнены книгами с неиспользованными билетами, которые водители выбрасывали в конце маршрута. При помощи дырокола я мог наделать своих билетов и путешествовать в любую точку Л.А., куда ходили автобусы. Вскоре я помнил расписания автобусов всей системы. Это был пример моей удивительной способности запоминать некоторые виды информации, сейчас я помню телефонные номера, пароли и другие вещи такие же далёкие, как и моё детство. Также в ранние годы открылась моя способность магического воздействия на людей. Когда я обнаружил, как работает новая уловка, я начал её отрабатывать, пока не достиг мастерства. Я находил некоторое удовольствие в одурачивании людей. Мой переход от телефонного фрикинга к хакингу произошёл в старших классах, когда я столкнулся с так называемой социальной инженерией и встретил другого студента, также увлечённого фрикингом. Телефонный фрикинг – это разновидность хакинга, когда вы исследуете телефонные сети, эксплуатируя телефонные системы и служащих телефонных компаний. Он показал мне некоторые уловки, которые он мог делать с телефонами, вроде получения любой информации телефонной компании о её клиентах и использования секретных те-

стовых номеров, чтобы делать бесплатные звонки на дальние расстояния. Бесплатные только для нас – намного позднее я узнал, что это были вовсе не секретные номера: счета приходили какому-нибудь абоненту MCI. Это было моё знакомство с социальной инженерией – мой детский сад, так сказать. Он и другой телефонный фрикер, которого я встретил позднее, давали мне послушать свои звонки в телефонную компанию. Я узнал, как заставить себя звучать убедительно и узнал о различных офисах и процедурах телефонной компании. Но это «обучение» продолжалось недолго. Вскоре я всё это делал сам, делая даже лучше, чем мои первые учителя. Направление моей жизни на ближайшие 15 лет было определено.

Одной из моих любимейших шуток был захват неавторизованного доступа к телефонному коммутатору и подмена класса телефонной службы моего товарища по фрикингу. Когда он хотел позвонить из дома, то получал сообщение опустить гривенник, потому что коммутатор телефонной компании воспринимал его телефон как общественный телефон-автомат.

Я изучал всё, что касается телефонов – не только электронику, коммутаторы и компьютеры, но также организацию корпорации, процедуры и терминологию. Вскоре я, возможно, знал о телефонной системе больше, чем любой из служащих.

И я развил мои навыки в социальной инженерии на-

столько, что к 17 годам я мог говорить с большинством из служащих Telco почти о чём угодно, лично или по телефону. Моя хакерская карьера началась в старшей школе. Тогда мы использовали термин хакер к человеку, который потратил огромное количество времени, копаясь с софтом и железом, разрабатывал более эффективные программы или исключал всё ненужное, чтобы сделать работу быстрее. Сейчас термин стал ругательством, означая «опасный преступник». Здесь я использую термин хакер в том же смысле, в каком он всегда использовался раньше, в более мягком смысле. В конце 1979 группа хакеров из Los Angeles Unified School District предложила мне взломать The Ark, компьютерную систему Digital Equipment Corporation, использовавшуюся для разработки софта для их операционной системы RSTS/E. Я хотел быть принятым в эту хакерскую группу, чтобы я мог узнать у них больше об операционных системах. Эти новые «друзья» знали номер диал-апа компьютерной системы DEC. Но они не могли войти без имени аккаунта и пароля. Когда вы кого-то недооцениваете, он может вернуться и ударить с фланга. В данном случае это был я, сумевший взломать систему DEC в столь юном возрасте. Представившись Антоном Черновым (Anton Chernoff), одним из ведущих разработчиков проекта, я просто позвонил системному администратору. Я заявил, что не могу войти в один из «моих» аккаунтов, и убедил этого парня

достаточно, чтобы он предоставил мне доступ и позволил мне выбрать пароль по своему усмотрению. В защите экстра класса любой пользователь, соединяющийся с системой, должен был ввести диал-ап пароль. Системный администратор дал мне его. Это был пароль «buffoon» (клоун), которым, я думаю, он себя почувствовал, когда стало понятно что произошло. Менее чем за 10 минут я получил доступ к RSTE/E системе DEC. И я вошёл не как обычный пользователь, у меня были все привилегии системного разработчика. Поначалу мои новые так называемые друзья не поверили, что я получил доступ к The Ark. Один из них отпихнул меня от клавиатуры с лицом, выражающим недоверие. Его рот открылся, когда он увидел, что я в привилегированном аккаунте. Позднее я обнаружил, что они начали копирование исходного кода компонентов к операционной системе DEC. Теперь была моя очередь удивляться. Когда они скопировали софт, они позвонили в отдел безопасности корпорации DEC и сказали, что кое-кто взломал корпоративную сеть компании. И выдали моё имя. Мои так называемые друзья сначала использовали мой доступ к исходному коду высокой секретности, а затем меня подставили.

Это был урок, и ещё не один такой урок мне пришлось выучить. Через несколько лет я неоднократно сталкивался с неприятностями, потому что я доверял людям, которых считал своими друзьями. После шко-

лы я изучал компьютеры в Обучающем Компьютерном Центре в Лос Анджелесе.

Через несколько месяцев мой школьный компьютерный администратор догадался, что я обнаружил уязвимость в их операционной системе и получил полные привилегии администратора на их миникомпьютере IBM. Лучшие компьютерные эксперты из их преподавательского штата не смогли найти как я это сделал. Это был один из моих ранних опытов «найма на работу». Мне сделали предложение, от которого я не смог отказаться: сделать почётный проект по повышению безопасности школьного компьютера или предстать перед обвинением во взломе системы. Конечно, я выбрал почётный проект и с Почестью закончил получение высшего образования в Cum Laude. Становясь социальными инженерами, некоторые встают каждое утро с постели, боясь своей каждодневной рабочей рутины. Я был достаточно удачлив, чтобы наслаждаться своей работой. Вы не можете себе представить вызов, награду и удовольствие, которые я испытывал, когда работал частным сыщиком. Я затачивал свои таланты в искусстве под названием социальная инженерия – заставляя людей делать вещи, которые они обычно не делают для незнакомцев, и получая за это деньги. Для меня было нетрудно стать профессионалом в социальной инженерии. Мой отец вышел из семьи потомственных торговцев, так что искусство

влияния и убеждения могло быть унаследованной чертой. Когда Вы объединяете склонность к обману людей с таланами влияния и убеждения, то достигаете профиля социального инженера. Вы могли бы сказать, что под эту классификацию попадают две специальности. Мошенник обманывает людей, чтобы забрать у них деньги. Социальный инженер обычно использует обман, влияние и убеждение, чтобы получить информацию. В то время, когда я проводил свои махинации с автобусными билетами, я был слишком мал, чтобы знать, что было плохого в том, что я делал. Я использовал талант, чтобы открывать секреты, которые не должен был знать. Я развивал этот талант, используя обман, умение заболтать людей, и развивая хорошо заточенные навыки манипулирования.

Чтобы развить навыки в моём ремесле (если я могу называть его ремеслом), я выбирал какой-нибудь кусок информации, неважно какой, и смотрел, мог ли мне его сообщить человек на другом конце телефонного провода. Через эти репетиции, вскоре я мог получить любую информацию, какую хотел. В Конгрессе, на эксперименте перед сенаторами Либерманом и Томпсоном я сказал: «Я получил неавторизованный доступ к компьютерным системам некоторых из крупнейших корпораций на планете и успешно проник в самые защищённые компьютерные системы. Чтобы получить исходные коды различных операционных систем и те-

лекоммуникационных устройств и изучить их внутреннее устройство и уязвимости, я использовал как технические, так и нетехнические навыки». Я искал секретную информацию об операционных системах, сотовых телефонах, только чтобы удовлетворить моё любопытство и убедиться, что я мог это сделать. Поток событий, изменивших мою жизнь, начался, когда я стал объектом статьи на титульном листе Нью-Йорк Таймс 4-го июля 1994 года.

Джон Марков (John Markoff) – медиа-мошенник

«Кевин Митник – взбесившийся компьютерный программист, использующий техническое колдовство и старое как мир мошенничество» (Нью-Йорк Таймс, 7/4/94). Используя старое как мир желание получить незаслуженное благосостояние, силу публичной лжи и дискредитирующие истории о своём объекте на титульном листе Нью-Йорк Таймс, Джон Марков был настоящим взбесившимся репортёром. Марков заработал более $ 1 млн., единолично создав то, что я называю «Мифом о Кевине Митнике.» Он стал очень богатым, используя ту же самую технологию, которую я использовал, чтобы компрометировать компьютерные системы и сети по всему миру: обман. Однако в данном случае жертвой обмана был не администратор системы или компьютерный пользователь, это был каждый, кто доверял новостям, опубликованным на страницах Нью-Йорк Таймс.

Самыйразыскиваемый в киберпространстве

Безусловно, статья Маркова в Таймс была специально написана, чтобы получить контракт на книгу об истории моей жизни. Я никогда не встречался с Марковым, всё же он буквально стал миллионером, благодаря его клеветническому и дискредитирующему «репортажу» обо мне в Таймс и его книге «Киберпанк» (1991) [1]. В статью он включил несколько десятков утверждений обо мне, которые приводились как факты без указания источников, и даже минимальная проверка (проведения которой, как я думал, требуют у своих репортёров все первоклассные газеты) показала бы их несоответствие. В этой ложной и дискредитирующей статье Марков заклеймил меня «самым разыскиваемым в киберпространстве» без указания причин и подтверждающих свидетельств, как автор какой-нибудь бульварной газеты. В своей клеветнической статье Марков ложно заявлял, что я перехитрил ФБР; что я взломал компьютеры в NORAD (которые даже не соединены ни с одной из внешних сетей); и что я был компьютерным «вандалом», не смотря на тот факт, что я не повредил ни одного компьютера преднамеренно. Эти и другие утверждения были полностью ложны и предназначены, чтобы вызвать страх по поводу моих способностей. В другом нарушении журналист-

---

[1] в русском переводе – «Хакеры» – прим.редактора

ской этики, в этой и всех последующих статьях обо мне Марков не смог скрыть личную враждебность за мой отказ участвовать в создании «Киберпанка». Кроме того, я стоил ему приличного потенциального дохода, отказавшись возобновить участие в фильме по мотивам книги. Также статья Маркова ясно предназначалась, чтобы уколоть американские правоохранительные агентства.

«… Кажется, силы правопорядка не способны поймать его …», писал Марков. Статья специально представляла меня как Общественного Врага Номер Один в киберпространстве, чтобы повлиять на Министерство Юстиции и поднять приоритет моего дела. Несколькими месяцами позже, нарушая закон и журналистскую этику, Марков и его кореш Тсутому Шимомура (Tsutomu Shimomura) участвовали в моём аресте как правительственные агенты. Оба были поблизости, когда для нелегального обыска моей квартиры и ареста использовали три неподписанных ордера. И во время расследования моей деятельности эти двое также нарушили закон, прервав мой телефонный звонок. Сделав меня злодеем, в своей последующей статье Марков представил Шимомуру как героя номер один в киберпространстве. Снова нарушая журналистскую этику и не раскрывая существовавшие ранее отношения: этот герой в течение нескольких лет был личным другом Маркова. Моё первое столкновение с Марко-

вым произошло в конце 80-х, когда он и его жена Кати Хафнер (Katie Hafner) связались со мной во время создания книги «Киберпанк», которая должна была стать историей о трёх хакерах: немецком юноше Пенго (Pengo), Роберте Моррисе и обо мне.

В чём была моя выгода от участия? Ни в чём. Я не видел причины рассказывать им свою историю, если они собирались на ней заработать, так что я отказался помочь. Марков выдвинул мне ультиматум: или интервью, или информация из любого источника будет воспринята как правда. Он был по-настоящему расстроен и разозлён оттого, что я не буду сотрудничать, и дал понять, что у него есть средства, чтобы заставить меня пожалеть об этом. Я стоял на своём и отказался сотрудничать, несмотря на давление. Опубликованная книга показывала меня как «Хакера с тёмной стороны». Я решил, что авторы преднамеренно включили неподтверждённые, ложные утверждения, чтобы отомстить мне за отказ. Придав моему символу зловещий вид и представив меня в чёрном свете, они, возможно, увеличили продажи книги. Однажды мне позвонил кинопродюсер с большими новостями: Голливуд заинтересовался фильмом о Хакере С Тёмной Стороны из Киберпанка. Я заявил, что история обо мне далека от истины, но он всё ещё был очень заворожен проектом. Я согласился на двухлетний контракт в $5000, плюс дополнительные $45000, если они доберутся до про-

изводства и дело сдвинется дальше. Когда срок контракта истёк, компания попросила о его продлении на 6 месяцев. К тому времени я нашёл выгодную работу, так что у меня было мало причин наблюдать за производством фильма, который показывал меня в таком неблагоприятном и ложном свете. Я отказался от продления. Это разрушило сделку с фильмом для всех, включая Маркова, который возможно ожидал от проекта огромного заработка. Это была ещё одна причина мстительного отношения Маркова ко мне. Когда «Киберпанк» был опубликован, у Маркова и его друга Шимимуры была переписка по email. Они оба подозрительно интересовались моим местонахождением и моей деятельностью. Удивительно, в одном e-mail сообщении содержалась информация, что я посещал Университет Невады в Лас Вегасе и пользовался студенческой компьютерной лабораторией. Могло ли это означать, что Марков и Шимомура собирались написать другую книгу обо мне? Иначе почему их волновало то, чем я занимался? Впоследствии Марков предпринял шаги, произошедшие в 1992 году.

Я приближался к концу моего условного заключения за взлом корпоративной сети Digital Equipment Corporation (DEC). Тем временем я узнал, что правительство готовило против меня другое дело за с проведение контрразведывательных действий по выяснению причины размещения телефонных жуч-

ков на телефонных линиях Лос-Анджелесской фирмы P.II. В своих раскопках я нашёл подтверждение моих подозрений: люди из службы безопасности Pacific Bell действительно исследовали фирму. Итак, в Лос-Анджелесском Окружном Департаменте Шерифа был сотрудник с компьютерным преступлением (по-совпадению этот сотрудник оказался братом-близнецом соавтора этой книги. Мир тесен.) Приблизительно в это время федералы внедрили своего информатора, чтобы он завёл меня в западню. Они знали, что я всегда старался держать козырные карты против любого агентства, которое за мной следило. Так что они сделали так, чтобы этот информатор вошёл ко мне в доверие и намекнул, что за мной наблюдают. Он также поделился со мной информацией о компьютерной системе, используемой в Pacific Bell, что позволило мне делать свои контр наблюдения. Когда я раскрыл его замыслы, я открыл свои карты и разоблачил его участие в мошенничестве с кредитными карточками во время его работы с правительством в качестве информатора.

Уверен, федералы оценили это! Моя жизнь изменилась в День Независимости 1994, когда рано утром меня разбудил мой пейджер. Звонивший сказал, чтобы я немедленно купил газету Нью-Йорк Таймс. Я не мог поверить, что Марков не только написал обо мне статью, но что Таймс поместила её на титульном листе. Первая мысль, пришедшая мне на ум, была о моей без-

опасности – теперь правительство существенно повысит свои усилия, чтобы меня найти. Меня обнадёжило то, что Таймс использовала очень неподходящую фотографию. Я не боялся, что меня узнают, потому что они выбрали настолько старую фотку, что она совсем не была на меня похожа! По мере прочтения статьи я понял, что Марков основывался на описании из своей книги о Кевине Митнике. Я просто не мог поверить, что Нью-Йорк Таймс рискнула напечатать его вопиюще ложные утверждения обо мне. Я чувствовал себя беспомощным. Даже если у меня будет возможность ответить, конечно, я не смогу собрать аудиторию, эквивалентную Нью-Йорк Таймс, чтобы опровергнуть возмутительную ложь Маркова. Я согласен, что мог быть болью в чьей-то заднице, но я никогда не уничтожал, не использовал против и никому не открывал полученную информацию. Фактические потери компаний от моей хакерской деятельности составляли стоимость телефонных звонков, которые я делал за их счёт, деньги, затраченные компаниями, чтобы закрыть уязвимости в безопасности, и в некоторых случаях, может быть, стоимость переустановки систем и приложений компаний из страха, что я мог модифицировать софт, чтобы использовать его для получения доступа в будущем. Эти компании оставались бы уязвимыми к более худшим взломам, если бы моя деятельность не предупредила о слабых местах в линии их защиты. Хотя я причинил

некоторые потери, мои действия и намерения не были злонамеренны… и Джон Марков изменил всемирное восприятие опасности, которую я представлял. Власть одного неэтичного репортёра из такой влиятельной газеты, пишущего лживую и дискредитирующую историю о ком угодно, может коснуться каждого из нас. Следующей целью можете быть вы.

После моего ареста меня перевезли в Окружную Тюрьму в Смитфилде в Северной Каролине, где приказом Службы Маршаллов США меня разместили в «the hole» – одиночной камере. Втечение недели федеральные обвинители и мой адвокат пришли к соглашению, от которого я не мог отказаться. Меня могли выпустить из одиночки при условии, что я откажусь от фундаментальных прав и соглашусь со следующим: а) никакого слушания залога; b) никакого предварительного слушания; и с) никаких телефонных звонков, кроме звонков моему адвокату и двум членам семьи. Подпись и я мог выйти из камеры. Я подписался.

Федеральные обвинители стояли за каждой злой шуткой, описанной в книге, пока я не вышел на свободу почти через 5 лет. Меня периодически заставляли отказаться от своих прав. Но ведь это было дело Кевина Митника: здесь нет правил. Никакого уважения к конституционным правам обвиняемого. Моё дело основывалось не на правосудии, а на стремлении правительства победить любой ценой. Обвинители представи-

ли суду значительно раздутые заявления об ущербе и угрозе, которую я представлял. Медиа повсюду разнесли цитирование этих утверждений, так что обвинителям было уже поздно отступать. Правительство не могло себе позволить проиграть дело Митника. Мир наблюдал.

Я уверен, что суд купился на страх, созданный медиа, так как многие этичные журналисты брали «факты» из уважаемой Нью-Йорк Таймс. Очевидно миф, созданный медиа, также испугал правоохранительных чиновников. В конфиденциальном документе, попавшем к моему адвокату, говорилось, что Служба Маршаллов США выпустила предупреждение ко всем правоохранительным агентам не показывать никаких личных данных обо мне; в противном случае они могут обнаружить, что их жизни электронно разрушены. Наша Конституция требует, чтобы до слушания обвиняемый считался невиновным, таким образом предоставляя всем гражданам право на слушание залога, на котором обвиняемый имеет возможность быть представленным жюри, предоставить доказательства и подвергнуть свидетелей перекрёстному допросу. Невероятно, что правительство смогло обойти эту защиту, основываясь на ложной истерии, распущенной безответственными репортёрами вроде Джона Маркова. Без прецедента меня содержали в тюрьме как человека, задержанного до суда или приговорённого более чем

к 4 с половиной годам заключения. Отказ судьи в слушании моего залога был полностью одобрен в Верховном Суде США. В конце концов, моя команда защиты посоветовала мне установить другой прецедент: я был первым федеральным задержанным в истории США, которому было отказано в слушании залога. По крайней мере, в этом случае федеральные обвинители не смогут утверждать, что я мог начать ядерную войну, просвистев в трубку таксофона, как делали другие федеральные обвинители в более ранних делах. Наиболее серьёзные обвинения были в том, что я скопировал находящийся в частной собственности исходный код для различных сотовых телефонных трубок и популярных операционных систем. Ещё, обвинители публично заявили, что я причинил некоторым компаниям суммарные потери более $300 млн. Детали о количестве потерь всё ещё находятся под охраной суда, возможно чтобы защитить вовлечённые компании; однако, моя группа защиты уверена, что запрос обвинителей о защите информации был произведён, чтобы прикрыть их грубое участие в моём деле. Стоит также отметить, что ни один из потерпевших не сообщил о потерях в Securities and Exchange Commission, как того требовал закон. Либо несколько межнациональных корпораций нарушили федеральный закон, обманув SEC, акционеров и аналитиков, либо потери, относящиеся к моему хакерскому делу были слишком

тривиальны, чтобы о них сообщать. В книге «Игра беглеца» (Fugitive Game) Джонатана Литтмана (Jonathan Littman) содержатся сообщения, что в пределах недели после истории на титульном листе Нью-Йорк Таймс агент Маркова получил «конверт с вознаграждением» от издателя Walt Disney Hyperion за книгу о кампании по моему задержанию. Вознаграждение оценивается в $750 000. Также по сведениям Литтмана Голливуд собирался снять кино и Miramax вручил ему более $200 000 за идею и «ещё $650 000 должны были выплатить к началу съёмок». Недавно конфиденциальный источник сообщил мне, что сделка Маркова оценивалась намного дороже, чем Литтман думал вначале. Так что Джон Марков стал миллионером, а я получил 5 лет. Одна из книг, в которой исследуются юридические аспекты моего дела, была написана человеком из Районной Прокуратуры Лос-Анджелеса, одним из моих обвинителей. В книге «Захватывающие компьютерные преступления» (Spectacular Computer Crimes) Бак Блумбекер (Buck Bloombecker) написал: «Меня огорчает то, что я вынужден писать о моих бывших коллегах в менее чем лестных терминах… Меня часто посещало признание Помощника Поверенного Соединённых Штатов Джеймса Асперджера (James Asperger), что большинство из аргументов, использовавшихся для содержания Митника за решёткой, основывались на слухах.» Дальше он говорит: «Доволь-

но плохо, что обвинения, сделанные в суде, распространялись газетами среди миллионов читателей по всей стране. Но хуже всего то, что эти несоответствующие заявления большей частью опирались на содержание Митника за решёткой без возможности выплатить залог». В статье в Форбс (Forbes) 1999 Адам Л. Пененберг (Adam L. Penenberg) красноречиво описал мою ситуацию: «Преступления Митника были безвредны. Он взломал компьютеры корпорации, но ни одна улика не доказывает, что он уничтожил данные. Или продал что-нибудь из того, что скопировал. Да, он воровал софт, но делая это, держал его при себе.» В статье говорится, что моё преступление было «гримасничаньем перед дорогостоящими системами безопасности, которые покупали большие корпорации.» В книге «Игра беглеца» автор Джонатан Литтман также замечает: «Жадность правительства можно понять. Но хакер, использующий свою власть для своей выгоды … это то, что они не могут поймать.» В другом смысле в той же книге Литтман пишет: Поверенный США Джеймс Сандерс (James Sanders) признался Судье Файлзеру (Judge Pfaelzer), что ущерб DEC от Митника был не $4 млн., как сообщали заголовки, а $160 000. Даже эта сумма содержала не стоимость ущерба, причинённого Митником, а грубые оценки затрат на поиск уязвимостей в безопасности DEC. Правительство подтвердило, что у него не было никаких дока-

зательств диких требований о содержании Митника в одиночном заключении без возможности выплатить залог. Никаких доказательств, что Митник когда-либо ставил под угрозу безопасность АНБ (NSA). Никаких доказательств, что Митник когда-либо распускал ложные сообщения о безопасности Pacific Bank. Никаких доказательств, что Митник когда-либо изменял кредитный счёт судьи. Но, возможно, под влиянием ужасных сообщений медиа судья отклонил просьбу Митника о сделке и приговорил его к более долгому заключению, чем требовало правительство. За годы моего хакерского хобби я получил неожиданную славу, обо мне написали бесчисленное количество газетных и журнальных статей и 4 книги. Клеветническая книга Маркова и Шимомуры легла в основе фильма «Takedown». Когда сценарий фильма был найден в Интернете, многие мои сторонники начали пикетирование Miramax Films, чтобы привлечь общественное внимание к моей ложной характеристике. Без помощи многих щедрых и справедливых людей кинофильм, конечно, изобразил бы меня как Ганнибала Лектора киберпространства (см. «Молчание ягнят», прим. перев.). Под давлением моих сторонников компания согласилась уладить дело, чтобы избежать судебного иска.

Финальные выводы

Несмотря на клеветническое и возмутительное описание Джона Маркова, мои преступления были простыми преступлениями в хакинге и фрикинге. С момента ареста все действия по отношению ко мне были незаконны, включая вмешательство в личную жизнь. Предположения, сделанные в статье Маркова без суждений, причин или доказательств, что я лишил кого-то денег, повредил компьютеры или мошенничал, были полностью лживы и не подтверждены свидетельствами. Мои преступления мотивировались любопытством: я хотел знать столько, сколько мог знать о работе телефонных сетей и о входах и выходах в компьютерной безопасности. Из ребёнка, который любил совершать магические уловки, я стал самым печально известным хакером в мире, которого боялись корпорации и правительство. Оглядываясь на последние 30 лет моей жизни, я допускаю, что, опираясь на моё любопытство, желание изучать технологию и хороший интеллектуальный вызов, я сделал несколько чрезвычайно плохих решений. Сейчас я стал другим человеком. Я обратил свои таланты и обширное знание, которое я собрал о безопасности и тактике социальной инженерии, на помощь правительству, компаниям и ин-

дивидуумам, чтобы обнаруживать и отвечать на угрозы информационной безопасности. Эта книга – ещё одна возможность использовать мой опыт, чтобы помочь другим избежать злонамеренных информационных воров. Думаю, что истории будут приятными, предупреждающими и поучительными.

Введение

Перевод: Minux (mariannaowen@pochta.ru)

Мы, люди, рождены со внутренним двигателем для изучения окружения. Будучи молодыми, Кевин Митник и я серьезно интересовались миром и страстно стремились самоутвердиться. Мы нередко были вознаграждены за наши попытки изучать новые вещи, решать загадки, а также побеждать в играх. Но в тоже самое время мир со своими правилами ограничивал свободу наших исследований. Для наших самых смелых ученых и технологических предпринимателей, а также людей подобных Кевину Митнику, следующих внутреннему зову ,предоставляют нам величайшие потрясения, позволяя нам завершить вещи, которые другим казались невозможными.

Кевин Митник – один из самых хороших людей, которых я знаю. Спросите его, и он откровенно скажет вам, что то, чем он занимался – социальная инженерия – включает в себя обман людей. Но Кевин уже не социальный инженер. И даже когда он им был, его целью никогда не было стать богатым или же нанести вред другим. Но это не говорит о том, что нет опасных и разрушительных преступников, которые используют социальную инженерию для нанесения вреда другим. Фак-

тически, это то из-за чего Кевин и написал эту книгу – чтобы предупредить вас о них.

«Искусство обмана» показывает насколько мы все уязвимы – правительство, бизнес, и каждый из нас лично – к вторжениям социальных инженеров. В этой сознательно-безопасной эре мы тратим огромные деньги на технологии защиты наших компьютерных сетей и данных. Эта книга показывает, как легко можно обманывать посвященных лиц и всю эту технологическую защиту.

Работаете ли вы в правительстве или же занимаетесь бизнесом, эта книга снабдит вас качественным планом, поможет вам понять, как социальные инженеры работают, и что вы можете сделать, чтобы помешать им. Используя придуманные истории, которые одновременно развлекают и просвещают, Кевин и его соавтор Билл Симон воплотили в жизнь технику социальной инженерии. После каждой истории они предлагают практические указания, чтобы помочь защититься нарушений и угроз, которые они описывают.

Технологические меры безопасности оставляют большие пробелы, которые люди, как Кевин, помогут вам закрыть. Прочитав эту книгу, вы поймете, что нам всем надо следовать советам Митника.

Стив Возняк

Предисловие

Перевод: Yarlan Zey (yarlan@pisem.net)

Некоторые хакеры стирают файлы или целые жёсткие диски – их называют *кракерами* или *вандалами* . Некоторые хакеры-новички не заботятся об изучении технологии, а просто скачивают хакерский инструментарий для взлома компьютерных систем – их называют *скрипт-кидди* . Более опытные хакеры с навыками в программировании разрабатывают хакерские программы и рассылают их по сетям и ББС. И ещё, есть индивиды, которые не интересуются технологией, но используют компьютер просто как средство для хищения денег, товаров и услуг.

Не смотря на созданный средствами массовой информации миф о Кевине Митнике, я – не злонамеренный хакер.

Но я начну всё по порядку.

С чего всё начиналось

Возможно, мой жизненный путь сложился ещё с раннего детства. Я был счастливым ребёнком, но меня мучала скука. После того как от нас ушёл отец, когда мне было три года, моя мать стала работать официанткой, чтобы прокормить нас. Тогда меня воспитывала одна мать, которая и так почти весь день тратила на изматывающую работу с сумасшедшим графиком, и я почти всё свободное время был предоставлен сам себе. Я сам был своей сиделкой.

Проживание в долине Сан-Фернандо открывало мне возможность для исследования всего Лос-Анджелеса, и к 12 годам я обнаружил способ, как можно путешествовать по огромной равнине Л.А. бесплатно. Однажды во время поездки в автобусе я понял, что вся защита купленных мной автобусных билетиков от подделки основывалась на уникальной модели бумажного дырокола, которым водитель отмечал на билете день, время и маршрут. Знакомый водитель, отвечая на мои тщательно сформулированные вопросы, сказал мне, где можно достать этот дырокол.

Предполагается, что со своим билетом вы можете пересесть на другой автобус и продолжить поездку в том же направлении, но я выработал метод, как можно

проехать куда угодно совершенно бесплатно. Для начала я отправился в автобусный парк за чистыми билетами.

Мусорные корзины у автобусного терминала всегда переполнены книгами с целой половиной неиспользованных билетов, которые водители выкидывали в конце маршрута. При помощи дырокола я мог наделать из чистых билетов своих собственных маршрутов и отправиться путешествовать в любую точку, куда ходили автобусы Л.А. Вскоре я помнил почти все расписания автобусов всей системы. (Это был первый пример моей удивительной памяти запоминать специфическую информацию. Сейчас я всё ещё помню телефонные номера, пароли и другие по-видимому, тривиальные вещи столь же далёкие как и моё детство).

Другим моим увлечением, также обнаруженным в раннем возрасте, была практическая магия (фокусы). Узнав, как действует та или иная уловка, я отрабатывал её много раз, пока не достигал совершенства. В какой-то степени именно через фокусы я открыл удовольствие от получения секретных знаний.

От телефонного фрикинга к хакингу

Впервые я столкнулся с тем, что позднее стал называть *социальной инженерией* , в средней школе, когда встретил другого школьника, также увлечённого хобби под названием телефонный фрикинг.

Это было моё вступление в социальную инженерию, так сказать. Мой друг и ещё один телефонный фрикер, которого я повстречал немного позднее, давали мне послушать свои спланированные звонки в телефонную компанию. Я услышал, что они говорили, чтобы казаться убедительными, я узнал о различных отделениях и процедурах телефонной компании. Но «обучение» длилось недолго . Вскоре я всё это делал сам, совершенствуясь в процессе, делая всё даже лучше моих первых учителей.

Итак, мой жизненный путь на ближайшие 15 лет был предначертан. В средней школе одной из моих излюбленных шуток был захват неавторизованного доступа к телефонному коммутатору и подмена класса услуги товарищей по фрикингу. Когда они пробовали позвонить из дома, электронный голос в трубке предлагал опустить четвертак, потому что коммутатор телефонной компании воспринимал звонок как звонок с платного таксофона.

Я стал жадно поглощать всё, что мог узнать о телефонах: не только об электронике, коммутаторах и компьютерах, но также всё о корпоративной организации, процедурах и терминологии. Вскоре я, возможно, знал о телефонной системе больше среднего служащего компании. И я развил навыки в социальной инженерии до такого уровня, что к 17 годам я мог разговаривать с работниками телефонной компании почти о чём угодно, без разницы – лично или по телефону.

Моя всем известная хакерская карьера фактически началась, когда я был в средней школе. Пока я не могу описать всё в деталях, достаточно сказать, что одной из движущих сил моих первых хаков было желание быть принятым в хакерскую группу.

Тогда мы ещё использовали термин хакер по отношению к индивиду, который потратил огромное количество времени, копаясь в софте и железе, либо разрабатывая более эффективные программы, либо обходя ненужные шаги, чтобы сделать работу быстрее. Сейчас термин стал бранным словом, означая «умышленный преступник». На этих страницах я использую термин хакер в том смысле, которым он всегда был – в его первоначальном значении.

После школы я изучал компьютеры в Учебном Компьютерном Центре в Лос-Анджелесе. Спустя несолько месяцев, школьный компьютерный администратор обнаружил, что я нашёл уязвимость в операционной си-

стеме и заполучил полные администраторские привилегии на их IBM миникомпьютере. Лучшие компьютерные эксперты из преподавательского штата не смогли понять, как я это сделал. Возможно, это был один из первых примеров, когда «хакера взяли на работу», мне сделали предложение, от которого я не мог отказаться: сделать почётный проект по улучшению безопасности школьного компьютера или иметь дело с обвинением в хакинге системы. Конечно, я выбрал почётный проект и с почестями закончил получение высшего образования.

Становление социальным инженером

Некоторые люди просыпаются каждое утро, боясь своей каждодневной рутины. Мне повезло – я наслаждался своей работой. Вы не можете себе представить вызов, награду и удовольствие, которые я испытывал, когда работал частным сыщиком. Я затачивал свои таланты в искусстве под названием *социальная инженерия* (заставляя людей делать вещи, которые они не стали бы обычно делать для незнакомца) и получая за это зарплату.

Для меня не было ничего сложного стать профессионалом в социальной инженерии. Мои предки со стороны отца были потомственными торговцами, поэтому искусство влияния и убеждения могло быть врождённой чертой. Когда вы объединяете эту черту и склонность к обману людей, вы получаете портрет типичного социального инженера.

Возможно, вы скажете, что искусству обмана соответствуют две рабочих специальности. Тот, кто надувает и обманывает людей за их деньги, относится к одной суб-специальности – это *мошенник* . Тот, кто использует обман, влияние и убеждение против компаний, целясь обычно в их информацию, относится к другой

суб-специальности – *социальный инженер* . Во времена моих трюков с автобусными билетиками, когда я был слишком молод, чтобы понять что-то неправильное в моих действиях, я начал использовать свой талант, чтобы узнавать секреты, к которым у меня, как предполагалось, не было доступа. Я опирался на этот талант, обман, знание терминологии и растущие навыки в манипуляции людьми.

Я работал над развитием навыков в моём ремесле, если я могу называть это ремеслом, следующим образом – я выбирал какой-нибудь кусок информации (любой, без разницы) и смотрел, мог ли я, разговаривая с кем-нибудь на другом конце телефонного провода, узнать это от него. Таким же образом я тренировался с фокусами. И через эти тренировки я вскоре обнаружил, что мог виртуально достать любую информацию, которую хотел.

Вот что я сказал на слушании в Конгрессе сенаторам Либерману и Томпсону несколько лет спустя:

Я получил неавторизованный доступ к компьютерным системам в некоторых крупнейших корпорациях на планете и успешно проникнул в некоторые наиболее гибкие когда-либо разрабатывавшиеся компьютерные системы. Чтобы достать исходные коды различных операционных систем и телекоммуникационных устройств для изучения их внутренней работы и уязвимостей, я использовал как технические,

так и нетехнические способы.

Вся эта деятельность была прямиком направлена на удовлетворение моего любопытства. Только ради того, чтобы узнать мог ли я это сделать, я добывал секретную информацию об операционных системах, сотовых телефонах и других вещах.

Финальные выводы

После ареста я подтвердил, что мои действия были незаконны, и что я совершал вторжения в личную жизнь.

Мои преступления мотивировались любопытством. Я хотел знать столько, сколько мог о том, как работают телефонные сети и входы-выходы в компьютерной безопасности. Из ребёнка, который любил показывать магические фокусы, я превратился в самого печально известного хакера в мире, которого боялись корпорации и правительство. Бросая взгляд на свою жизнь за последние 30 лет, я признаю, что, идя на поводу у любопытства, желания изучать технологию и интеллектуального вызова, я принял несколько чрезвычайно плохих решений,

Сейчас я изменился. Я обратил свои таланты и обширные знания об информационной безопасности и тактике социальной инженерии на помощь правительству, бизнесу и индивидам, чтобы помочь им предотвращать, обнаруживать и отвечать на угрозы информационной безопасности.

Эта книга – ещё одна возможность использовать мой опыт, чтобы помочь другим людям избежать злонамеренных информационных воров. Я надеюсь, вы най-

дёте истории приятными и поучительными.

Вступление

Перевод: Yarlan Zey (yarlan@pisem.net)

Эта книга содержит исчерпывающие сведения об информационной безопасности и социальной инженерии. Чтобы помочь вам, здесь даны основные элементы структуры книги:

В первой части я покажу самое слабое звено в безопасности и объясню, почему вы и ваша компания подвержены риску атак социальных инженеров.

Во второй части вы увидите, как социальные инженеры используют вашу доверчивость, ваше желание быть полезным, вашу симпатию и ваше человеческое легковерие, чтобы получить то, что они хотят. Вымышленные истории о типичных атаках продемонстрируют, что социальные инженеры могут носить множество шляп и множество лиц. Если вы думаете, что вы никогда с ними не сталкивались, возможно, вы ошибаетесь. Вполне возможно в этих историях вы узнаете сценарии, которые уже испытали на себе, и удивитесь, если окажется, что вы сталкивались с социальной инженерией. Но, прочитав главы со второй по девятую, вы будете знать что делать, когда услышите телефонный звонок следующего социального инженера.

Третья часть – это часть, в которой вы увидите, как

социальный инженер достигает своей цели. В вымышленных историях показывается, как он может проникнуть в ваше корпоративное здание, украсть секреты, от которых зависит ваша компания, и обойти все ваши высокотехнологичные меры безопасности. Из сценариев этого раздела вы узнаете, что угрозы, могут варьироваться от простой мести служащего до кибертерроризма. Если вы цените информацию, которая держит ваш бизнес на плаву, и секретность ваших данных, вы захотите прочитать главы с десятой по четырнадцатую от начала до конца.

Важно отметить, что если это не оговорено специально, все истории из книги полностью вымышлены.

В четвёртой части я читаю корпоративную лекцию, как предотвратить успешные атаки социальных инженеров на вашу организацию. Глава 15 содержит макет эффективной программы по обучению безопасности. И Глава 16, возможно, спасёт вашу шею – это последовательная политика безопасности, которую вы можете настроить для вашей организации и сразу же применить для защиты компании и информации.

Наконец, я предоставил раздел «Защищайтесь сразу», который включает в себя контрольные списки, таблицы и диаграммы. Они объединяют ключевую информацию, которую вы можете использовать на работе, чтобы помочь вашим служащим отражать атаки социальных инженеров.

Повсюду в книге вы также найдёте несколько полезных элементов: ссылки lingo, которые расшифровывают определения и терминологию хакеров и социальных инженеров, Сообщения Митника, короткие ценные заметки, которые помогут усилить вашу стратегию безопасности, и примечания, дающие дополнительную информацию.

Глава 1: Самое слабое звено в безопасности

Перевод: Yarlan Zey (yarlan@pisem.net)

Компания может приобрести лучшие технологии по безопасности, какие только можно купить за деньги, натренировать своих людей так, что они станут прятать все свои секреты, прежде чем пойти ночью домой, и нанять охранников в лучшей охранной фирме на рынке.

Но эта компания всё ещё остаётся полностью Уязвимой.

Сами люди могут полностью следовать лучшей практике по безопасности, рекомендованной экспертами, по-рабски устанавливать каждый вновь появившийся рекомендованный программный продукт по безопасности и тщательно следить за конфигурацией своей системы и следить за выпуском патчей.

Но и они всё равно полностью уязвимы.

Человеческий фактор

Не так давно, давая показания перед Конгрессом, я объяснял, что часто я получал пароли и другие кусочки секретной информации компаний, просто притворяясь кем-нибудь и спрашивая о них.

Это естественно – стремиться к абсолютной безопасности, но это желание заставляет многих людей соглашаться с ложным чувством защищённости. Рассмотрим ответственного и любящего отца семейства, у которого есть Medico – надёжный замок в парадной двери, который ограждает его жену и детей и его дом. Сейчас он спокоен, так как сделал свою семью гораздо более защищённой от вторжений. Но как насчёт грабителя, который разбивает окно или взламывает код у замка на двери гаража? Тогда нужно установить охранную систему? Неплохо, но всё же недостаточно. Независимо от того, насколько дороги замки, домовладелец остаётся уязвим.

Почему? Потому что человеческий фактор по-настоящему самое слабое звено в безопасности.

Безопасность слишком часто просто иллюзия и иногда иллюзия может быть даже хуже легковерия, наивности или невежества. Самый знаменитый в мире учёный 20 века Альберт Эйнштейн говорил: «Можно быть

уверенным только в двух вещах: существовании вселенной и человеческой глупости, и я не совсем уверен насчёт первой». В конце концов, атаки социальных инженеров успешны, когда люди глупы или, гораздо чаще, просто неосведомлены о хороших мерах безопасности. Аналогично нашему домовладельцу, многие профессионалы в информационных технологиях (ИТ) придерживаются неправильных представлений, будто они сделали свои компании в значительной степени неуязвимыми к атакам, потому что они используют стандартные продукты по безопасности: файрволлы, системы для обнаружения вторжений (IDS) или серьёзные устройства для аутентификации, такие как биометрические смарт-карты или time-based tokens. Любой, кто думает, что одни только эти продукты по безопасности предоставляют достаточную защиту, соглашается на иллюзию защиты. Это как жить в мире фантазий – неизбежно, рано или поздно он столкнётся с инцидентом, связанным с безопасностью.

Как заметил консультант по безопасности Брюс Шнайер: «Безопасность – это не продукт, это процесс». Кроме того, безопасность – это не технологическая проблема, это проблема людей и управления.

Пока разработчики непрерывно изобретают всё лучшие и лучшие технологии защиты, делая всё более трудным возможность использовать технические уязвимости, атакующие всё чаще используют человече-

ский фактор. Зачастую очень просто взломать человеческий файрволл, все затраты не превышают стоимости одного телефонного звонка и атакующий подвержен минимальному риску.

Классический случай обмана

Какая самая большая угроза безопасности ваших деловых активов? Ответ прост – это социальный инженер – нечестный фокусник, который заставляет вас смотреть на его левую руку, пока правой ворует ваши секреты. Этот персонаж часто так дружелюбен и любезен, что вы благодарны за то, что с ним столкнулись.

Далее рассмотрим пример социальной инженерии. Немногие люди сегодня всё ещё помнят молодого человека по имени Стенли Марк Рифкин и его маленькое приключение с ныне уже несуществующим Тихоокеанским Национальным Банком в Лос-Анджелесе. Подробности его авантюры противоречивы и Рифкин (как и я) никогда не рассказывал свою историю, поэтому следующее основано только на печатных источниках.

Взлом кода

Однажды в 1978 году Рифкин заглянул в помещение банка для телеграфных переводов с табличкой «только для авторизованного персонала», в котором служащие каждый день получали и отправляли трансферты в несколько миллиардов долларов.

Он работал с этой компанией по контракту и занимался разработкой системы для резервного копирования данных из этого помещения на случай, если ко-

гда-нибудь произойдёт сбой их главного компьютера. Эта роль давала ему доступ к процедурам передачи трансфертов, включая возможность наблюдать, что делали служащие банка для совершения операций. Он узнал, что служащие банка, уполномоченные на передачу трансфертов, каждое утро получали тщательно охраняемый код, используемый при осуществлении запросов.

В телеграфном помещении работали некоторые служащие, которые не утруждали себя попытками запомнить новый код, изменявшийся каждый день. Они записывали код на кусочек бумаги и клали его куда-нибудь в поле зрения. В этот особенный ноябрьский день Рифкин зашёл в это помещение со специальным визитом. Он хотел взглянуть на этот кусочек бумаги.

Зайдя в комнату, он немного повозился со своей работой, удостоверившись, что система резервного копирования правильно работает с основной системой. Тем временем он незаметно прочитал и запомнил код на прилепленном кусочке бумаги. Несколько минут спустя он вышел. Как он позже рассказывал, он чувствовал себя, словно выиграл лотерею.

Счёт в швейцарском банке…

Покинув комнату около 3-х часов по полудню, он направился прямиком к платному таксофону в мраморном холле здания, в который опустил монету и набрал номер помещения для трансфертов. Затем он сменил

шляпу, трансформируясь из Стенли Рифкина, банковского консультанта, в Майкла Хансена, служащего Международного Отдела банка.

Согласно одному из источников, разговор происходил следующим образом:

«Привет, это Майк Хансен из международного», сказал он молодой женщине, которая подняла трубку.

Она запросила офисный номер. Эта была стандартная процедура, и он был к ней готов: «286» ответил он.

Девушка ответила: «ОК, ваш код?»

Рифкин говорил, что в этот момент его переполненное адреналином сердцебиение «поднялось до максимальной точки». Он медленно ответил: «4789». Затем он дал инструкции для перевода: «ровно 10 миллионов 200 тысяч долларов» для Компании Ирвин-Траст в Нью-Йорке в качестве кредита в Банк Wozchod Handels в Цюрихе, Швейцария, в котором у него уже был открыт счёт.

Затем девушка ответила: «ОК, готово. Сейчас мне нужен внутриофисный номер».

Сердце Рифкина ёкнуло, это был вопрос, которого он не ожидал, кое—что ускользнуло из его внимания во время подготовки. Но он решил оставаться в роли, действуя как будто всё было нормально, и спокойно ответил без всякого замешательства: «Дай проверить, я перезвоню тебе позже». Он опять сменил шляпу и позвонил в другое отделение банка, в этот раз, предста-

вляясь работником из помещения для трансфертов. Он получил нужный номер и опять позвонил девушке.

Она приняла номер и сказала «Спасибо» (При тех обстоятельствах её благодарность, должно быть, выглядела ироничной.)

Заслуживая скрытность

Несколькими днями позже Рифкин прилетел в Швейцарию, забрал свои деньги и обменял в российском агентстве более $8 миллионов на горстку алмазов. Затем он улетел обратно, прошёл через таможню США, спрятав алмазы в поясе для денег. Он осуществил крупнейший грабёж банка в истории и сделал это без всякого оружия, даже без компьютера. Странно, но в конечном счете, запись о нём попала в *Книгу мировых рекордов Гиннеса* под категорией «крупнейшее компьютерное мошенничество».

Стенли Рифкин использовал искусство обмана – навыки и технику, которая сегодня зовётся социальной инженерией. Скрупулёзный план и хорошо подвешенный язык – всё, что для этого нужно.

И это то, о чём эта книга – о технике социальной инженерии (в которой ваш покорный слуга – профессионал) и о том, как защититься от её использования против вашей компании.

Характер угрозы

История Рифкина прекрасно описывает, насколько мы можем заблуждаться в своём ощущении безопасности. Инциденты вроде этого – хорошо, может быть стоимостью не в $10 миллионов, но, тем не менее, болезненные инциденты – случаются *каждый день* . Возможно, прямо сейчас вы тоже теряете свои деньги или кто-то сейчас ворует планы касательно новой продукции, и вы об этом даже не подозреваете. Если это ещё не случилось с вашей компанией, под вопросом остается только: не случится ли это вообще, а *когда именно* .

Растущее беспокойство

В своём обзоре по компьютерным преступлениям за 2001 год Институт Компьютерной Безопасности сообщил, что 85% опрашиваемых организаций сталкивались с нарушениями компьютерной безопасности за последние 12 месяцев. Это поразительные данные: только 15 организаций из 100 смогли ответить, что у них не было нарушений безопасности в течение года. Столь же поразительным было число организаций, которые ответили, что имели финансовые потери из-за компьютерных нарушений: 64%. Более половины организаций понесли финансовые потери. *И всего за один*

год .

Мой собственный опыт подсказывает мне, что числа в отчётах вроде этих несколько раздуты. Я с подозрением отношусь к людям, которые делают обзор. Но это не повод говорить, что ущерб не обширен, он на самом деле огромен. Тот, кто не предвидит инцидента с безопасностью, думает заранее неверно.

Коммерческие продукты по безопасности, применяемые в большинстве компаний, главным образом нацелены на защиту от любительского компьютерного вторжения, вроде тех, совершаемых юнцами, известными как скрипт-кидди. Фактически, эти дети, скачивающие программное обеспечение и мечтающие стать хакерами, в большинстве случаев просто неприятность. Гораздо большие потери и реальные угрозы происходят от корыстных налётчиков, у которых есть чётко сформулированные цели, и которые мотивируются финансовой выгодой. Эти люди фокусируются на одной цели, в отличие от любителей, которые пытаются просканировать как можно больше систем. В то время как компьютерный налётчик-любитель работает над количеством, профессионал целится в информацию в зависимости от её ценности и качества.

Технологии, вроде устройств для аутентификации (для проверки идентичности), контроля доступа (для управления доступом к файлам и системным ресурсам), и системы для обнаружения вторжений (элек-

тронный эквивалент сигнализации) необходимы для программы корпоративной безопасности. И всё же, на сегодняшний день для компании типичнее потратить больше денег на кофе, чем на развёртывание контрмер для защиты организации против атак на безопасность.

Точно так же, как мозг преступника не может сопротивляться искушению, мозг хакера стремится найти окружной путь вокруг мощных технологических средств защиты. И во многих случаях они этого достигают, целясь в людей, которые пользуются технологиями.

Методы введения в заблуждение

Есть популярное высказывание, что безопасный компьютер это тот, который выключен. Умно, но неверно: *преступник* может просто попросить кого-нибудь зайти в офис и включить этот компьютер. Если противник захочет получить вашу информацию, он это сделает, обычно любым из нескольких возможных способов. Это только вопрос времени, терпения, индивидуальных черт и упорства. Вот когда искусство обмана вступает в силу.

Для того, чтобы обойти средства безопасности, налётчик, захватчик или социальный инженер должен найти способ обмануть доверенного пользователя, раскрыть информацию или незаметно заставить неподозревающего человека дать ему доступ. Поскольку

возможны ситуации, когда доверенный пользователь обманут, подвержен влиянию, то есть его спровоцировали выдать секретную информацию или выполнить действия, создающие уязвимость в безопасности, в которую нападающий мог бы проскользнуть, то во всём мире не найдется таких технологий, которые могли бы защитить бизнес. Так же как криптоанализ может иногда расшифровать текст закодированного сообщения путём обнаружения слабого места в технологии шифрования, социальные инженеры могут использовать обман против ваших работников, чтобы обойти технологии защиты.

Злоупотребление доверием

Во многих случаях, успешные социальные инженеры обладают сильными человеческими качествами. Они очаровательны, вежливы и просты – социальные качества, необходимые для установления быстрой связи и доверия. Опытный социальный инженер может получить доступ к любой возможной информации, используя стратегию и тактику своего ремесла.

Здравомыслящие технологи кропотливо разработали решения по информационной безопасности для минимизации рисков, связанных с использованием компьютеров, но всё же оставили наиболее значимую уязвимость – человеческий фактор. Несмотря на интеллект, мы люди – вы, я и любой другой – остаёмся самой серьёзной угрозой для любой другой защиты.

Наш национальный характер

Никто из нас не задумывается об угрозе, особенно в западном мире. В Соединённых Штатах в особенности, нас никогда не учили подозревать друг друга. Нас учили «любить соседей» и доверять и верить друг другу. Посмотрите, как организациям по наблюдению за окрестностями трудно заставить людей запирать их дома и автомобили. Эта уязвимость очевидна, но всё же, кажется, игнорируется многими из тех, кто предпо-

читает жить в мире фантазий – до тех пор, пока не «случится пожар».

Мы знаем, что не все люди добрые и честные, но слишком часто мы поступаем таким образом, будто это неправда. Эта прекрасная невинность – образ жизни американцев, и слишком болезненно от него отказываться. Мы включили в нашу концепцию свободы, что лучшее место для жизни находиться там, где меньше всего нужны замки и ключи.

Большинство людей думают, что их никто не обманет, опираясь на веру, что возможность быть обманутым очень низка; налётчик, понимая эту общую уверенность, заставляет свои вопросы звучать столь разумно, что они не вызывают никаких подозрений за всё время эксплуатации доверия жертвы.

Организационная невинность

Эта невинность – часть нашего национального характера, очевидно, оказала большое влияние, когда компьютеры впервые стали соединяться между собой. Вспомните, что сеть ARPANet (Сеть Агентства Перспективных Исследований Департамента Обороны) предшественник Интернета, была разработана как средство для обмена исследовательской информацией между правительственными, исследовательскими и образовательными учреждениями. Целью была свобода информации, так же как и технологический прорыв. Поэтому многие образовательные учреждения устана-

вливали свои первые компьютерные системы с минимальной или даже вовсе с отсутствующей безопасностью. Один известный либертарианец программного обеспечения Ричард Залман даже отказывался защищать свой аккаунт паролем.

Но когда Интернет стал использоваться для электронной коммерции, опасность слабой безопасности электронного мира стала драматична. При этом, применение всё более усложняющихся технологий не решит проблему человеческой безопасности.

Напимер, посмотрите на наши аэропорты сегодня. Безопасность стала первостепенной, все же СМИ рассказывают нам о пассажирах, которые смогли обойти защиту и пронести потенциальное оружие через контрольные точки. Как это стало возможным в то время, когда наши аэропорты находятся в состоянии повышенного внимания? Неужели металло-детекторы ошиблись? Нет. Проблема не в машинах. Проблема – человеческий фактор: в людях, дополняющих машины. Должностные лица аэропорта могут сажать на каждый самолёт специальных маршаллов из национальной гвардии и установить металло-детекторы и системы по распознаванию лиц, но обучение сотрудников из службы безопасности у линии фронта как правильно обыскивать пассажиров могло бы помочь гораздо лучше.

Та же проблема существует в правительственных, бизнес – и образовательных учреждениях по всему ми-

ру. Не смотря на усилия профессионалов из безопасности, информация повсеместно остаётся уязвимой, и будет оставаться целью налётчиков с навыками в социальной инженерии до тех пор, пока не будет усилено самое слабое звено в безопасности – человеческое звено.

Сейчас больше, чем когда-либо, мы должны научиться перестать думать самонадеянно и побольше узнать о методах, которые пробуют использовать те, кто совершает атаки на конфиденциальность, целостность и работоспособность наших компьютерных систем и сетей.

Угроза взлома, который нарушит секретность вашей жизни или информационной системы вашей компании может казаться не настолько реальной, пока это не произойдёт однажды. Чтобы избежать столь дорогостоящей дозы действительности, нам нужно стать осведомлёнными, образованными, бдительными и настойчиво защищать наши информационные активы, нашу собственную персональную информацию и наши национальные критичные инфраструктуры. И мы должны научиться этому уже сегодня.

Террористы и обман

Конечно, обман это не эксклюзивное оружие социального инженера. Физический терроризм выходит на повестку дня и сейчас мы должны признать как никогда, что мир это опасное место. Цивилизация, в конце концов, только тонкая фанера.

Атаки на Нью-Йорк и Вашингтон, Округ Колумбия, в сентябре 2001 вселили печаль и страх в сердце каждого из нас – не только американцев, но и людей всех наций. Сейчас мы столкнулись с реальностью и знаем, что в любой точке планеты есть одержимые террористы, хорошо обученные и только ожидающие возможности начать атаку против нас.

Недавние усилия нашего правительства повысили уровень нашего осознания безопасности. Нам нужно оставаться на взводе, начеку против любых форм терроризма. Нам нужно понять, как террористы предательски изготавливают ложные удостоверения, играют роль студентов или соседей и проникают в толпу. Они скрывают свои истинные взгляды, устраивая против нас заговор – осуществляя фокусы с обманом, похожие на те, о которых вы прочитаете на этих страницах.

И пока, насколько я знаю, террористы ещё не ис-

пользовали уловки социальной инженерии для проникновения в корпорации, плотины, электростанции или другие жизненные компоненты нашей национальной инфраструктуры, их возможность всё равно остаётся. Понимание безопасности и правила безопасности, я надеюсь, благодаря этой книге, будут достаточно скоро приняты к месту и взяты на вооружение главными управляющими структурами.

Об этой книге

Корпоративная безопасность – это вопрос баланса. Слишком низкая безопасность делает вашу компанию уязвимой, но излишний упор на безопасность приводит замедлению роста и процветания компании. Задача состоит в нахождении баланса между защищённостью и эффективностью.

Другие книги по корпоративной безопасности фокусируются на технологиях аппаратного и программного обеспечения и, соответственно, недостаточно широко охватывают главную угрозу безопасности: обман человека. Цель этой книги, по сравнению с ними, заключается в том, чтобы помочь вам понять как вами, вашими сослуживцами и другими людьми из вашей компании могут манипулировать, и избежать риска стать жертвой. В основном книга концентрируется на нетехнических методах, которые враждебные налётчики используют для воровства информации, компрометации целостности информации, которая на первый взгляд безопасна, но на самом деле таковой не является, или уничтожения рабочего продукта компании.

Моя задача гораздо сложнее. Это сразу понятно из следующего: каждый читатель будет подвержен манипулированию со стороны величайших экспертов всех

времён в социальной инженерии – их родителям. Они найдут любые способы заставить вас сделать «для вашего же блага» то, что они сами считают лучшим. Родители становятся столь убедительными так же, как социальные инженеры умело выдумывают вероятные истории, причины и суждения для достижений своих целей. Да, каждого из нас наши родители обводили вокруг пальца: доброжелательные (и иногда не столь доброжелательные) социальные инженеры.

Выросшие в этих условиях, мы становимся уязвимыми к манипулированию. Нам жилось бы очень тяжело, если бы мы всё время стояли начеку, были недоверчивыми к другим, уверенными, что кто-нибудь может нас обмануть, чтобы нас провести. В идеальном мире мы бы слепо верили друг другу, верили, что люди, с которыми мы сталкиваемся, собираются быть честными и правдивыми. Но мы живём не в идеальном мире, и поэтому мы должны быть бдительны, чтобы отразить попытки противников ввести нас в заблуждение.

Основные части это книги, – части 2 и 3, – составлены из вымышленных историй, которые покажут вам социальных инженеров в действии. В этих разделах вы прочитаете о следующем:

Что телефонные фрикеры обнаружили несколько лет назад – гибкий метод получения неизвестных телефонных номеров у телефонной компании.

О нескольких различных методах, используемых на-

падающими, и не вызывающих тревоги даже у подозрительных служащих во время выдачи их компьютерных имён и паролей.

Как менеджер операционного центра сотрудничал с налётчиком, позволив ему украсть самую секретную информацию о продукте компании.

Методах налётчика, который обманул даму, заставив ее скачать и установить программное обеспечение, которое шпионит за набираемыми клавишами и отсылает ему по е-мейлу различные детали.

Как частные сыщики получают информацию о вашей компании и вашу персональную информацию. Это, я могу гарантировать, вызовет у вас мурашки на спине.

Возможно, вы подумаете, читая некоторые из историй во второй и третьей частях, что они нереальны, но ещё никто не смог преуспеть в противодействии лжи, грязным уловкам и схемам, описанным на этих страницах. Действительность состоит в том, что в каждом случае эти истории изображают события, которые могут и на самом деле происходят; многие из них каждый день происходят где-нибудь на планете, возможно даже с вашим собственным бизнесом, пока вы читаете эту книгу.

Материал в этой книге будет действительно разоблачительным, когда он станет защищать ваш бизнес, но также защитит вас лично от попыток социального

инженера нарушить целостность информации в вашей частной жизни.

В четвёртой части книги я сменил тему. Здесь моя цель помочь вам разработать необходимые бизнес-правила и тренинги, чтобы минимизировать риски ваших работников быть обманутыми социальным инженером. Понимание стратегии, методов и тактики социального инженера поможет вам подготовиться к применению разумных средств управления для охраны ваших ИТ активов без подрыва эффективности вашей компании.

Короче говоря, я написал эту книгу, чтобы повысить вашу осведомлённость о серьёзности угроз, исходящих от социальной инженерии, и помочь вам стать уверенней, что ваша компания и работники в меньшей степени будут подвержены угрозе с этой стороны.

Или, возможно, я должен сказать, гораздо меньше будут подвержены *снова* .

Глава 2: Когда безвредная информация опасна

Перевод: Yarlan Zey (yarlan@pisem.net)

Что большинство людей считает настоящей угрозой, исходящей от социальных инженеров? Что вам следует делать, чтобы быть на страже?

Если целью является получение какого-нибудь очень ценного приза – скажем, важного компонента интеллектуальной собственности компании, тогда, возможно, всё что нужно – это просто более недоступное хранилище и более тяжело вооруженные охранники. Правильно?

Но в жизни проникновение плохого парня через защиту компании часто начинается с получения какого-нибудь фрагмента информации или какого-нибудь документа, которые кажутся такими безвредными, такими обычными и незначительными, что большинство людей в организации не нашли бы причин почему им следовало бы её защищать и ограничивать к ней доступ.

Скрытая ценность информации

Многое из кажущейся безвредной информации, находящейся во владении компании, ценно для социального инженера, потому что может сыграть существенную роль в его попытке прикрыться плащом правдоподобности.

На страницах этой главы я буду вам показывать, что делают социальные инженеры, чтобы добиться успеха. Вы станете «свидетелем» атак, сможете, время от времени наблюдать действие с точки зрения атакуемой жертвы и, становясь на их место, оценить как бы вы (или, может быть, один из ваших работников или сослуживцев) сами могли себя повести. Во многих случаях вы также увидите эти же события с перспективы социального инженера.

В первой истории речь пойдёт об уязвимости в финансовой индустрии.

CREDITCHEX

В течение долгого времени британцы имели дело с очень консервативной банковской системой. Вы как обычный добропорядочный гражданин не могли просто зайти с улицы и открыть банковский счёт. Нет, банк не рассматривал вас в качестве своего клиента, пока какой-нибудь уже хорошо зарекомендовавший себя клиент не даст вам своё рекомендательное письмо.

Несомненно, это очень сильно отличается от сегодняшнего банковского мира. И наша современная лёгкость в совершении сделок нигде так не развита, как в дружелюбной, демократичной Америке, где почти кто угодно может зайти в банк и легко открыть расчётный счёт, правильно? Да, но не совсем. На самом деле, банки не желают открывать счёт для кого-нибудь, кто может иметь за собой ситуации с неоплаченными счетами – это всё равно, что соглашаться на грабёж. Поэтому для многих банков стала стандартной практика быстрой оценки перспектив нового клиента.

Одной из больших компаний, которые предоставляют банкам такую информацию, является CreditChex (все названия изменены). Они предоставляют своим клиентам ценную услугу, но, как и многие компании, также могут, не подозревая об этом, стать источником

информации для социальных инженеров.

Первый звонок: Ким Эндрюс

«Национальный Банк, это Ким. Вы хотели открыть сегодня счёт?»

«Привет, Ким. У меня есть к вам вопрос. Вы пользуетесь CreditChex?»

«Да.»

«Когда вы звоните в CreditChex, номер, который вы им даёте – это „Merchant ID"?»

Пауза. Она взвешивала вопрос, удивляясь, к чему это всё, и следует ли ей отвечать.

Звонивший быстро продолжил, не теряя времени:

«Потому что, Ким, я работаю над книгой. Это касается частных исследований.»

«Да», сказала она, отвечая на вопрос под воздействием новых обстоятельств, польщённая тем, что помогает писателю.

«Итак, это называется Merchant ID, правильно?»

«Эээ, ага.»

«ОК, отлично. Я хотел убедиться, что примечание в книге правильно. Спасибо за помощь. До свидания, Ким.»

Второй звонок: Крис Тэлберт

«Национальный банк, новые счета, это Крис.»

«Привет, Крис. Это Алекс», ответил звонивший. «Я из отдела обслуживания клиентов CreditChex. Мы делаем обзор по улучшению нашей службы. У вас есть

для меня пара минут?»

Она была рада помочь, и звонивший продолжил:

«ОК, в какие часы ваш отдел открыт?» Она ответила и продолжала отвечать на его список вопросов.

«Сколько служащих в вашем отделении пользуются нашей службой?»

«Как часто вы звоните нам с запросами?»

«Какой из наших номеров 800– вы используете для звонков?»

«Наши представители всегда были вежливы?»

«Сколько времени занимает наш ответ?»

«Как давно вы работаете в банке?»

«Какой Merchant ID вы сейчас используете?»

«Вы когда-нибудь обнаруживали неточности в информации, которую мы вам предоставляем?»

«Есть ли у вас советы по улучшению нашей службы?»

И:

«Вы не могли бы заполнить наши периодические анкеты с вопросами, которые мы пришлём в ваш отдел?»

Она согласилась, они ещё немного поболтали, незнакомец повесил трубку, и Крис вернулась к работе.

Третий звонок: Генри МакКинси

«CreditChex, это Генри МакКинси, чем могу вам помочь?»

Звонивший сказал, что он из Национального Банка. Он назвал текущий Merchant ID и имя и номер соци-

ального страхования человека, о котором он искал информацию. Генри спросил дату рождения и звонивший сказал её тоже.

Через несколько секунд Генри прочитал список с экрана компьютера.

«Уэллс Фарго – есть сообщения о NSF однажды в 1998-м, в $2 066.» NSF – это недостаточные фонды – типичный банковский термин, касающийся чеков, которые были выписаны, когда на счету не хватало денег, чтобы их покрыть.

«Что-нибудь ещё после этого?»

«Ничего.»

«Были ли ещё какие-нибудь запросы?»

«Сейчас посмотрю. Да, два, оба в прошлом месяце. Третий Объединённый Кредитный Союз Чикаго.» Он наткнулся на следующее имя, Взаимные Инвестиции Шенектеди. «Это в штате Нью-Йорк», добавил он.

Частный сыщик в действии

Все три из этих звонков были сделаны одним человеком – частным сыщиком, которого мы будем называть Оскар Грейс. У Грейса появился новый клиент, один из первых. Ещё несколько месяцев назад он был полицейским. Он обнаружил, что кое-что в его новой работе добывалось обычным путём, но некоторая часть бросала вызов его ресурсами и изобретательности.

Популярные писатели любовных романов Сэм Спейдс и Филипп Марлоус проводили длинные ночи, сидя в машинах и следя за нечестными супругами. Частные сыщики в реальной жизни делают то же самое. Они также делают более обыденные, но не менее важные слежки за враждующими супругами. Большей частью они основываются на навыках в социальной инженерии, чем на борьбе с бессонницей с прибором ночного видения.

Новым клиентом Грейса была леди, и по виду своего платья и ожерелья довольно обеспеченная. Однажды она зашла в его офис и села в кожаное кресло, единственное, на котором не было сложенной кипы газет. Она поставила на стол свою сумочку от Гуччи, повернув логотипом в его направлении, и заявила, что хочет

сказать своему мужу о том, что хочет развода, но есть «только одна маленькая проблема».

Кажется, её муженёк был на шаг впереди. Он уже снял все наличные с их сберегательного счёта и даже гораздо большую сумму с их брокерского счёта. Она хотела знать, куда подевались их активы, и сказала, что её адвокат по разводу не смог вообще ничем помочь. Грейс предположил, что адвокат был одним из тех юристов, которые сидят на верхних этажах небоскрёбов и не желают пачкать свои руки ни в чём грязном, например, разбираясь, куда исчезли её деньги.

Не мог бы Грейс помочь?

Он уверил её, что это будет непросто, назвал примерную цену, накладные расходы и получил чек в качестве аванса.

Затем он столкнулся с проблемой. Что вы делаете, если вам никогда прежде не поручали подобную работу и даже не знаете с чего начать искать денежный след? Вы как ребёнок делаете первые шаги. Вот история Грейса согласно нашему источнику.

Я знал о CreditChex, и как банки им пользуются – моя бывшая жена работала в банке. Но я не знал терминов и процедур, и спрашивать её об этом было бы пустой тратой времени.

Шаг первый: Разузнать о терминологии и выяснить, как сделать запрос так, чтобы он звучал, как будто я знаю, о чём говорю. Первая молодая леди Ким в банке,

в который я позвонил, была настроена подозрительно, когда я спросил, как они идентифицируют себя, когда звонят в CreditChex. Она колебалась, она не знала, стоит ли мне это говорить. Было ли это моим поражением? Нисколько. Фактически, колебание дало мне важный знак, что я должен сообщить причину, которой бы она поверила. Когда я обманул её, сказав, что провожу исследования для книги, это уменьшило её подозрения. Скажите, что вы писатель или сценарист и вам любой откроется.

У неё была информация, которая могла бы помочь – вроде необходимых данных, которые требует CreditChex относительно человека, о котором вы делаете запрос; о чём вы можете спрашивать; и главное, банковский номер Merchant ID Ким.

LINGO

Сжигать источник – считается, что нападающий сжигает источник, когда он даёт жертве понять, что атака имела место. Как только жертва узнаёт об этом и сообщает другим служащим или руководству о попытке, становится невероятно сложно использовать тот же источник для будущих атак.

Вы вынуждены опираться только на инстинкт, чутко вслушиваясь, что и как жертва говорит. Эта леди звучала достаточно настороженно и могла что-нибудь заподозрить, если бы я задавал много необычных вопросов. Даже притом, что она не знала, кто я и с какого но-

мера я звоню, нельзя вызывать подозрительности, потому что вы вряд ли захотите сжигать источник – возможно, вы захотите позвонить в этот офис в другой раз.

Я всегда слежу за маленькими знаками, которые дают понять, насколько человек поддаётся сотрудничеству. Это может варьироваться от «Вы располагаете к себе, и я верю всему, что вы говорите» до «Вызвать полицию, поднять Национальную Гвардию, этот парень замышляет что-то нехорошее».

Я понял, что Ким находится на грани последнего, поэтому я просто позвонил кому-нибудь из другого отдела. Мой следующий звонок свёл меня с Крис, с ней уловка сработала. В этот раз тактика заключалась в том, чтобы спрятать важные вопросы среди несущественных, которые служат, чтобы вызвать чувство доверия. Прежде чем я задал вопрос о номере Merchant ID в CreditChex, я провел небольшой тест, задав ей личный вопрос о том, как долго она работает в банке.

Личный вопрос – это как скрытая мина, некоторые люди переступают через него, не замечая; для других она взрывается и взывает в защите. Поэтому если я задаю личный вопрос и она отвечает, и тон её голоса не меняется, это означает, что, возможно, она не относится подозрительно к природе вопроса. После этого я могу спокойно задать нужный вопрос, не вызывая у неё подозрений, и она скорее всего даст мне необходимый ответ.

Есть ещё одна вещь, о которой знают частные сыщики: никогда не заканчивать разговор сразу после получения нужной информации. Ещё два-три вопроса, немного болтовни и только тогда можно прощаться. Позже, если жертва вспомнит о чём вы спрашивали, это скорее всего будет пара последних вопросов. Остальные обычно забываются.

Итак, Крис дала мне её номер Merchant ID и телефонный номер, по которому они делают запросы. Я хотел задать ещё несколько вопросов, чтобы узнать, как много информации можно узнать от CreditChex. Но лучше было не рисковать.

Теперь я мог в любое время позвонить в CreditChex и получить информацию. При таком повороте событий служащий CreditChex был счастлив поделиться со мной точной информацией касающихся двух мест, в которых муж моей клиентки недавно открыл счета. Итак, куда же подевались деньги, которые разыскивала его потенциальная бывшая жена? Ещё куда-нибудь, кроме банковских учреждений, о которых сообщил парень из CreditChex?

Анализ обмана

Весь этот фокус основывался на единственной фундаментальной тактике социальной инженерии: получение доступа к информации, которую работники компании считают безвредной, когда на самом деле она опасна.

Первая банковская служащая подтвердила термин для описания номера идентификации, используемого для звонков в CreditChex: Merchant ID. Вторая выдала телефонный номер для звонков в CreditChex и самый важный кусок информации: номер Merchant ID банка. Вся эта информация казалась клерку безвредной. В конце концов, ведь банковская служащая думала, что она говорит с кем-то из CreditChex – так что плохого было в раскрытии номера?

Всё это было положено в основу для третьего звонка. У Грейса было всё необходимое, чтобы позвонить в CreditChex. Он представился служащим одного из банков-клиентов, – Национального банка, – и просто спросил всё, что нужно.

Помимо хороших навыков в краже информации, которыми обладает любой хороший карманник, Грейс обладал талантом незаметно угадывать настроение людей. Он знал об обычной тактике прятанья ключевых вопросов среди безвредных. Он знал, что личный вопрос проверит второго клера на желание сотрудничать, прежде чем спрашивать о номере Merchant ID.

Ошибку первого служащего, касающуюся подтверждения терминологии номера ID CreditChex, практически невозможно предотвратить. Эта информация столь широко известна в банковской индустрии, что кажется незначительной – хорошая модель безвредной информации. Но второй служащей, Крис, не следова-

ло отвечать на вопросы без проверки, действительно ли звонивший был тем, кем назвался. По крайней мере, ей следовало спросить у него имя и номер, чтобы перезвонить. В этом случае атакующему было бы намного труднее замаскироваться под представителя CreditChex.

Сообщение от Митника

В этой ситуации Merchant ID – аналог пароля. Если бы персонал банка относился к нему как к ATM PIN, они бы лучше оценивали критичность природы этой информации. А в вашей организации есть внутренний номер, к которому люди относятся без особой осторожности?

Для звонков в CreditChex было бы лучше использовать что-нибудь другое, вместо номера, сообщаемого звонившим, чтобы проверить действительно ли этот человек работает там, и действительно ли компания обрабатывает запросы своего клиента. Однако, учитывая практику настоящего мира и временной прессинг, в котором сегодня работают многие люди, этой проверки по телефону достаточно кроме случаев, когда служащий подозревает, что совершается атака.

Западня для инженера

Широко известно, что агентства по трудоустройству (т.н. охотники за головами) пользуются социальным инженерингом, чтобы переманивать корпоративные таланты. Вот пример того, как это может происходить.

В конце 1990-х одно не слишком этичное агентство подписало контракт с новым клиентом – компанией, ищущей инженеров-электронщиков с опытом в области телефонной промышленности. Исполнителем проекта стала леди с чувственным низким голосом и сексуальными манерами, которая научилась их использовать, чтобы вызывать первоначальные доверие и привязанность по телефону.

Леди решила организовать набег на провайдера услуг сотовой связи, чтобы посмотреть, можно ли было там найти несколько инженеров, которые могли бы поддаться соблазну перейти к конкуренту. Она не могла просто позвонить в центр связи и сказать: «Дайте мне поговорить с кем-нибудь с пятилетним опытом работы инженером.» Вместо этого по понятным причинам она начала охоту за талантами с поиска кусочков информации, которые кажутся совсем незначительными, информации, которую люди из компании скажут почти любому, кто спросит.

Первый звонок: Регистратор

Атакующая, пользуясь именем Диди Сэндс, сделала звонок в корпоративный офис по обслуживанию сотовых телефонов. Частично беседа проходила следующим образом:

Регистратор: Добрый вечер. Это Мари, чем я могу Вам помочь?

Диди: Вы можете соединить меня с Отделом Транспортировок?

Р: Я не уверена, что у нас есть такой, я посмотрю в справочнике. Это кто звонит?

Д: Это Диди.

Р: Вы находитесь в здании или…?

Д: Нет.

Р: Диди кто?

Д: Диди Сэндс. У меня был номер Транспортировки, но я его забыла.

Р: Один момент.

В этот момент, чтобы смягчить подозрения Диди случайно спросила, только ради того, чтобы дать понять, что она была «внутри», и знакома с местоположением компании.

Д: Вы в каком здании – Лейквью или Мэйн Плэйс?

Р: Мэйн Плэйс. *(пауза)* Вот: 805 555 6469.

Чтобы обеспечить себя запасным вариантом на случай если звонок в Транспортный отдел не даст то, что она искала, Диди также сказала, что она хочет погово-

рить с отделом по недвижимости. И регистратор так же дала ей этот номер. Когда Диди попросила соединить её с Транспортным, регистратор попробовала, но линия была занята.

Тогда Диди попросила *третий* номер – отдела работы со счетами – расположенного в штаб-квартире корпорации в Остине, Техас. Регистратор попросила подождать и отключилась от линии. Она сообщила в службу безопасности, что получила подозрительный телефонный звонок, и подумала, что происходит что-то странное. Это была небольшая, но типичная неприятность обыденной работы регистратора. Примерно через минуту регистратор вернулась на линию, посмотрела номер Счётного отдела и подключила Диди.

Второй звонок: Пэгги

Следующий разговор проходил следующим образом:

Пэгги: Счётный отдел, Пэгги.

Диди: Привет, Пэгги. Это Диди из Thousand Oaks.

П: Привет, Диди.

Д: Как дела?

П: Отлично.

Затем Диди воспользовалась знакомым термином в корпоративном мире, который означает код оплаты для назначения расходов из бюджета определённой организации или рабочей группы:

Д: Превосходно. У меня есть для тебя вопрос. Как

мне найти расчётный центр того или иного отдела?

П: Вы лучше бы обратились к бюджетному аналитику отдела (бухгалтеру).

Д: А Вы не знаете кто сейчас бюджетный аналитик в штаб-квартире Thousand Oaks? Я пытаюсь заполнить форму, но не знаю что это за расчётный центр.

П: Я знаю только, что Вам нужен номер расчётного центра, позвоните своему бюджетному аналитику.

Д: А у вашего отдела в Техасе есть свой расчётный центр?

П: У нас есть свой расчётный центр, но они не выдают полный список.

Д: Сколько цифр в этом расчётном центре? Ну, например, какой у Вас номер расчётного центра?

П: Хорошо, а Вы из 9WC или из SAT?

Диди не имела никаких представлений об этих отделах или группах, но это ничего не значило. Она ответила:

Д: 9WC.

П: Тогда там обычно 4 цифры. Откуда Вы, Вы сказали?

Д: Штаб-квартира – Thousand Oaks.

П: Хорошо, вот один для Thousand Oaks. 1A5N, Н – как в Нэнси.

Всего лишь поболтав достаточно долго с кем-нибудь, желающим быть полезным, Диди заполучила номер расчётного центра, который ей был нужен – один

из тех кусочков информации, которые никто не думает защищать, потому что он не может представлять какую-нибудь ценность для постороннего.

Третий звонок: Полезный неправильный номер

Следующий шаг Диди должен был превратить номер расчётного центра в нечто по-настоящему ценное.

Она начала со звонка в Отдел по Недвижимости, притворившись, что попала на неправильный номер. Начав с «Извините за беспокойство, но …», она заявила, что она была служащей, которая потеряла свой корпоративный справочник, и спросила, не он ли звонил насчёт новой копии. Человек ответил, что печатная копия уже устарела, потому что всё это доступно на корпоративном сайте.

Диди сказала, что предпочитает пользоваться бумажной копией, и человек посоветовал ей позвонить в Издательство, а потом, возможно, только чтобы ещё немного поболтать с сексуально-звучащей леди по телефону, услужливо посмотрел номер и дал ей.

Четвёртый звонок: Барт из Издательства

В Издательстве она поговорила с человеком по имени Барт. Диди сказала, что она была из Thousand Oaks, и у них появился новый консультант, которому нужна была копия справочника компании. Она сказала, что печатная копия была бы предпочтительнее, даже если она будет немного устаревшей. Барт сказал, что она должна заполнить форму реквизиции и прислать ему.

Диди сказала, что у неё нет под рукой форм, и не мог бы Барт любезно заполнить форму за неё? Он согласился с не слишком большим энтузиазмом, и Диди сообщила ему данные. Вместо адреса вымышленного подрядчика она сообщила номер, которые социальные инженеры называют *сбросом почты* , в данном случае адрес почтовой компании, в которой её компания арендовала почтовые ящики специально для ситуаций вроде этой.

Теперь вместо работы лопатой нужно было потрудиться ручками: Нужен был расчётный центр, в который придёт счёт за доставку справочника. Прекрасно – Диди дала расчётный центр для Thousand Oaks:

«IA5N, Н – как в Нэнси.»

Несколькими днями позже, когда прибыл корпоративный справочник, Диди обнаружила, что он был даже большей наградой, чем она ожидала: В нем не только был список с именами и телефонами, но также показывалось кто на кого работал – корпоративная структура целой организации.

Леди с хриплым голосом была готова начать охоту за головами, делая набеги при помощи телефонных звонков. Она умыкнула информацию, которая была необходима для начала набега, пользуясь хорошо подвешенным языком, который наточен до зеркального блеска у любого социального инженера.

LINGO

Сброс почты – термин социального инженера касательно почтового ящика, обычно арендованного на вымышленное имя, который используется для доставки документов или посылок обманутой жертвы.

Сообщение от Митника

Подобно кусочкам паззла, каждый кусок информации может быть несущественным сам по себе. Однако когда эти куски соединяются вместе, появляется ясная картина. В данном случае картиной, которую увидел социальный инженер, была полная внутренняя структура компании.

Анализ обмана

Эту атаку социального инженера Диди начала с получения телефонных номеров трёх отделов в компании. Это было легко, потому что спрашиваемые номера не были секретны, особенно для служащих. Социальный инженер учится звучать как посвящённое лицо, и Диди преуспела в этой игре. Один из телефонных номеров привёл её к номеру расчётного центра, который она затем использовала, чтобы получить копию справочника работников фирмы. Основные инструменты, которые ей были нужны: звучать дружелюбно, пользоваться корпоративной лексикой, и, в случае с последней жертвой, небольшой флирт.

И ещё один инструмент, существенный элемент, который нелегко достаётся – навыки социального инженера в манипулировании, появляющиеся после об-

ширной практики и неписаных уроков доверенных лю-
дей прошлых поколений.

Ещё одна «ничего не стоящая» информация

Помимо номера расчётного центра и внутренних номеров, какая еще, по-видимому, бесполезная информация может быть чрезвычайно ценной для вашего врага?

Телефонный звонок Питера Абеля

«Привет», сказал человек на другом конце линии. «Это Том из Parkhurst Travel. Ваш билет в Сан-Франциско готов. Вы хотите, чтобы Вам его доставили или Вы хотите забрать его сами?»

«Сан-Франциско?» сказал Питер. «Я не собираюсь в Сан-Франциско.»

«Это Питер Абель?»

«Да, но у меня не намечается никаких поездок.»

«Хорошо», сказал звонивший с дружелюбным смехом, «Вы уверены, что вы не собираетесь ехать в Сан-Франциско?»

«Если Вы сомневаетесь, вы можете поговорить с моим боссом…», сказал Питер, подыгрывая дружеской беседе.

«Звучит как путаница», ответил звонивший. «В нашей системе мы заказываем билеты, ссылаясь на номера работников. Возможно, кто-то использовал не-

правильный номер. Какой у Вас номер служащего?»

Питер любезно сказал свой номер. А почему нет? Он пишет его почти на каждой персональной форме, когда их заполняет, многие люди в компании имеют к нему доступ – человеческие ресурсы, платёжные ведомости и, очевидно, внешние транспортные агентства. Никто не относится к номеру работника как к чему-то секретному. Так какая разница?

Ответ нетрудно предсказать. Два или три куска информации – это иногда всё, что нужно для эффективного превращения, когда социальный инженер скрывается под чьей-то персоной. Узнать имя работника, его телефонный номер, его номер работника и, возможно, на всякий случай, имя и телефон его начальника, – и тогда компетентный социальный инженер будет знать почти всё, что ему нужно, чтобы звучать правдоподобно, когда он позвонит его следующей жертве.

Если бы вчера позвонил кто-нибудь и сказал, что он был из другого отдела вашей компании, и, учитывая вероятную причину, спросил ваш номер работника, вы бы отказались его сообщить?

А, между прочим, какой у Вас номер социального страхования?

Сообщение от Митника

Мораль этой истории такова: не выдавайте никакую личную или внутрикорпоративную информацию или идентификаторы любому, если вы не узнаёте его или

её голос.

Предотвращение обмана

Ваша компания ответственна за то, чтобы предупредить работников насколько серьёзной может быть выдача непубличной информации. Хорошая продуманная информационная политика безопасности вместе с надлежащим обучением и тренировками улучшат понимание работников о надлежащей работе с корпоративной бизнес-информацией. Политика классификации данных поможет вам осуществить надлежащий контроль за раскрытием информации. Без политики классификации данных вся внутренняя информация должна рассматриваться как конфиденциальная, если не определено иначе.

Примите к сведению эти шаги для защиты вашей компании от распространения кажущейся безвредной информации:

Отдел информационной защиты должен проводить обучения, детализуя методы, используемые социальными инженерами. Один метод, описанный выше, касается получения кажущейся нечувствительной информации и использование её для получения краткосрочного доверия. Каждый работник должен знать, что когда у звонящего есть знания о процедурах компании, лексике и внутренних идентификаторах, он дол-

жен подтвердить личность звонящего или получить от него разрешение на получение того, что он хочет. Звонящий может быть обычным работником или подрядчиком с необходимой внутренней информацией. Соответственно, на каждой корпорации лежит ответственность за определение соответствующего опознавательного метода, для использования в случаях, когда работники взаимодействуют с людьми, которых не могут узнать по телефону.

Человек или люди, ответственные за составление политики классификации данных, должны исследовать типы данных, которые кажутся безвредными и могут быть использованы законными служащими для получения доступа, но могут привести к получению важной информации. Хотя вы никогда не открыли бы коды доступа к вашей карте АТМ, вы сказали бы кому-нибудь, какой сервер вы используете для разработки программных продуктов? Может ли кто-нибудь, притворяющийся кем-то с законным доступом к корпоративной сети, использовать эту информацию?

Иногда одно только знание внутренней терминологии может заставить социального инженера казаться авторитетным и хорошо осведомлённым. Часто атакующий полагается на это общее неправильное представление, чтобы добиться согласия его/её жертвы. Например, Merchant ID – это идентификатор, который люди из Отдела Новых Счетов банка небрежно исполь-

зуют каждый день. Но такой идентификатор то же самое, что пароль. Если каждый работник будет понимать природу этого идентификатора, что он предназначен для подтверждения подлинности, он будет относиться к нему с большим уважением.

Сообщение от Митника

Согласно старой пословице: даже у настоящих параноиков, возможно, есть враги. Мы должны согласиться, что у любого бизнеса тоже есть враги – атакующие, которые целятся в инфраструктуру сети, чтобы скомпрометировать бизнес-секреты. Недостаточно просто ознакомиться со статистикой по компьютерным преступлениям – пришло время поддерживать необходимую обороноспособность, осуществляя надлежащее средство управления через хорошо известные политики и процедуры безопасности.

Ни одна компания – хорошо, по крайней мере, очень немногие – дают прямые номера своих CEO или председателей правления. Однако большинство компаний не беспокоятся о выдаче телефонных номеров большинства отделов и рабочих групп в организации – особенно кому-то, кто кажется или на самом деле является служащим. Возможная контрмера: осуществить политику, которая запрещает выдачу посторонним внутренних телефонных номеров работников, подрядчиков, консультантов и других. Ещё важнее разработать пошаговую процедуру для выяснения действительно

ли звонящий, спрашивающий о номерах, является настоящим служащим.

Коды рабочих групп и отделов, также как и копии корпоративных справочников (не важно, печатная копия, файл данных или электронная телефонная книга) частые цели социальных инженеров. Любой компании нужна письменная, хорошо разработанная политика касательно открытия информации этого типа. Нужно также завести учетную книгу записей, в которую будут записываться случаи, когда важная информация открывалась людям вне компании.

Информацию, вроде номера работника, не стоит использовать для аутентификации саму по себе. Любой работник должен быть обучен проверять не только личность, но и разрешение на получение информации.

В своем обучении безопасности предусмотрите обучение работников следующим подходам: всякий раз, когда незнакомец задаёт вопрос, научитесь сначала вежливо отключаться, пока запрос не будет проверен. Затем, прежде подтвердив его личность, следуйте политикам и процедурам компании, с уважением относясь к проверке и раскрытию непубличной информации. Этот стиль может идти вразрез нашему естественному желанию помочь другим, но небольшая здоровая паранойя может оказаться полезной, чтобы не стать следующей жертвой социального инженера.

Как показано в историях в этой главе, кажущаяся

безвредной информация может быть ключом к самым существенным секретам компании.

Глава 3: Прямая атака: просто попроси

Перевод: Artem (artemsib@inbox.ru)

Многие атаки социальной инженерии являются сложными, включая в себя тщательно планируемый ряд шагов, сочетая манипуляцию и технологические знания.

Но меня всегда поражает, как искусный социальный инженер может достичь своей цели с помощью простой прямой атаки. Как вы увидите, все, что может понадобиться – просто попросить информацию.

Случай с центром назначения линий

Хотите узнать чей-нибудь неопубликованный номер телефона? Социальный инженер может сообщить вам полдюжины способов (некоторые из них вы найдете в других историях книги), но, возможно, самым простым из них будет обычный телефонный звонок, как этот.

Номер, пожалуйста

Атакующий позвонил по неофициальному номеру телефонной компании, в механизированный центр назначения линий (Mechanized Line Assignment Center). Он сказал женщине, поднявшей трубку:

«Это Пол Энтони, кабельный монтер. Послушайте, здесь загорелась распределительная коробка. Полицейские считают, кто-то пытался поджечь собственный дом, чтобы получить страховку. Я остался здесь заново монтировать целый терминал из двухсот пар. Мне сейчас очень нужна помощь. Какое оборудование должно работать по адресу Саут-Мэйн (South Main), 6723?»

В других подразделениях компании человек, которому позвонили, должен знать, что сведения о неопубликованных номерах предоставляются только уполномоченным лицам. Предполагается, что о центре известно

только служащим компании. И если информация никогда не оглашалась, кто мог отказать в помощи сотруднику компании, выполняющему тяжелую работу? Она сочувствовала ему, у нее самой были нелегкие дни на работе, и она немного нарушила правила, чтобы помочь коллеге с решением проблемы. Она сообщила ему действующий номер и адрес для каждой из кабельных пар.

Сообщение от Митника

В человеческой натуре заложено доверять, особенно когда просьба кажется обоснованной. Социальные инженеры используют это, чтобы эксплуатировать свои жертвы и достичь своих целей.

Анализ обмана

Вы заметите, что в этих историях знание терминологии компании, ее структуры – различных офисов и подразделений, что делает каждое из них и какой информацией владеет – часть ценного багажа приемов успешного социального инженера.

Юноша в бегах

Человек, которого мы назовем Фрэнк Парсонс, был в бегах долгие годы, находясь в федеральном розыске за участие в подпольной антивоенной группировке в 1960-х гг. В ресторанах он сидел лицом к дверям и периодически оглядывался, что смущало других людей. Он переезжал каждые несколько лет.

В некоторый момент времени Фрэнк остановился в городе, который не знал, и приступил к поиску работы. Для таких как Фрэнк, с его развитыми компьютерными навыками (и навыками социального инженера, хотя он никогда не упоминал об этом при соискании) поиск хорошей работы обычно не составляет проблемы. За исключением случаев, когда организация ограничена в средствах, люди с хорошими компьютерными навыками обычно пользуются высоким спросом и им несложно обосноваться. Фрэнк быстро нашел высокооплачиваемое, постоянное место работы рядом со своим домом.

Просто объявление, подумал он. Но когда он начал заполнять анкеты, то столкнулся с неожиданностью. Работодатель требовал от соискателя предоставить копию криминальной характеристики, которую он должен был принести сам из полиции штата. Пачка доку-

ментов включала в себя бланк с местом для отпечатков пальцев. Даже если требовался только отпечаток правого указательного пальца, но его сверили бы с отпечатком из базы данных ФБР, то вскоре ему пришлось бы работать в продовольственной службе федеральной тюрьмы (приюта).

С другой стороны, Фрэнку пришло в голову, что он мог бы избежать этого. Возможно, образцы отпечатков пальцев не отправлялись из штата в ФБР. Как он мог выяснить это?

Как? Он был социальным инженером – как, вы думаете, он разузнал это? Он позвонил в патруль штата: «Привет. Мы выполняем исследование для министерства юстиции. Мы изучаем требования к новой системе идентификации отпечатков пальцев. Могу я поговорить с кем-нибудь, кто действительно разбирается в этом, и мог бы нам помочь?»

Когда к телефону подошел местный специалист, Фрэнк задал ряд вопросов о том, какие системы они используют, о возможностях исследования и хранения отпечатков пальцев. Были у них проблемы с оборудованием? Связаны они с картотекой отпечатков национального информационного центра или работают в пределах штата? Является ли оборудование достаточно простым для всех, кто обучается его использованию?

Ответ был музыкой для его ушей: они не связаны

с национальным центром, они только сверяются по криминальной базе данных штата (Criminal Information Index).

Сообщение от Митника

Сообразительные похитители информации не стесняются звонить должностным лицам из органов штата, федеральных и местных органов, чтобы узнать о процедурах правоприменения. Располагая такой информацией, социальный инженер может обойти типовые проверки безопасности вашей компании.

Это было все, что нужно было знать Фрэнку. На него не было записей в этом штате, поэтому он заполнил анкету, был принят на работу, и никто не появился однажды у его стола со словами: «Это джентльмены из ФБР, они хотят немного поговорить с вами».

И, по его словам, он показал себя образцовым служащим.

На пороге

Несмотря на миф о безбумажном офисе, компании продолжают печатать стопки бумаг каждый день. Печатная информация в в вашей компании может быть уязвимой, даже если вы предпринимаете меры предосторожности и помечаете ее как конфиденциальную.

Вот одна история, показывающая, как социальные инженеры могут получить ваши самые секретные документы.

Обман с номерами обратного вызова

Каждый год телефонная компания издает справочник тестовых номеров (или по крайней мере издавали, но, поскольку я все еще нахожусь под надзором, то не собираюсь спрашивать об этом). Этот документ высоко ценился фрикерами, так как содержал список тщательно скрываемых телефонных номеров, которые использовались мастерами, техниками и другими работниками компании для таких вещей как тестирование магистрали или проверки всегда занятых номеров.

Один из таких тестовых номеров, называемых на профессиональном языке «Loop-Around» (номер обратного вызова), был особенно полезен. Фрикеры использовали его как способ бесплатно поговорить друг с другом. Фрикеры также использовали его как

номер обратного вызова, чтобы дать его, например, в банке. Социальный инженер сообщал кому-нибудь в банке телефонный номер в своем офисе. Когда из банка звонили по тестовый номеру, фрикер мог получить звонок, кроме того, по этому номеру его не могли выследить.

В справочнике тестовых номеров содержал информацию, в которой нуждался фрикер. Поэтому, когда издавались новые справочники, они разыскивались множеством подростков, для которых любимым занятием было исследовать телефонную сеть.

Сообщение от Митника

Обучение безопасности в рамках политики компании по защите информации должно проводиться для всех сотрудников, а не только для служащих, у которых есть электронный или физический доступ к ИТ-активам компании.

Афера Стива

Конечно, телефонные компании не допускают свободного распространения этих книг, поэтому фрикерам приходится быть изобретательными. Как они делают это? Энергичный подросток, разыскивающий справочник , может разыграть такой сценарий.

Тихим осенним вечером в южной Калифорнии, парень, которого я назову Стив, звонит в центральный офис небольшой телефонной компании, здание, от которого отходят телефонные линии ко всем домам и

фирмам в зоне обслуживания.

Когда дежурный электромонтер отвечает на звонок, Стив заявляет, что он из подразделения компании, которое издает и распространяет печатные материалы. «У нас есть новый справочник тестовых номеров, – говорит он. – Но из соображений безопасности мы не можем отдать ваш экземпляр, пока не получим старый. Посыльный будет позже. Если вы хотите, оставьте ваш экземпляр прямо за дверью, он может заехать, забрать его и положить новый».

Ничего не подозревающему электромонтеру это кажется разумным. Он делает так, как его попросили, кладет на пороге здания свой справочник, на обложке которого ясно написано большими красными буквами: «**СЕКРЕТНЫЙ ДОКУМЕНТ КОМПАНИИ** . В СЛУЧАЕ НЕНАДОБНОСТИ УНИЧТОЖИТЬ».

Стив приезжает и осторожно оглядывается вокруг в поисках полицейских или сотрудников службы безопасности компании, которые могли спрятаться за деревьями, или ждать его в припаркованных машинах. Никого в поле зрения. Он небрежно берет справочник и уезжает.

Заговаривание зубов (Отвлекающая болтовня)

Не только активы компании находятся под угрозой сценария социальной инженерии. Иногда жертвами являются клиенты компании.

Работа по обслуживанию клиентов несет с собой отчасти разочарование, отчасти смех, отчасти невинные ошибки, которые могут привести к плохим последствиям для клиентов компании.

История Дженни Эктон

Дженни Эктон более трех лет работала в службе клиентов компании «Hometown Electric Power» в Вашингтоне, округ Колумбия. Она считалась одним из лучших служащих, проворной и добросовестной.

Была Неделя благодарения, когда раздался этот звонок. Звонящий сказал: «Это Эдуардо из отдела счетов (BIling department). У меня на проводе дама, секретарь исполнительных органов, работающих для одного из вице-президентов, она запрашивает информацию, но у меня не работает компьютер. Я получил письмо от девушки из кадровой службы, в котором было написано „ILOVEYOU“. Когда я открыл вложение, то не мог больше работать на своем компьютере. Вирус. Я подхватил дурацкий вирус. Не могли бы вы найти для ме-

ня некоторые сведения о клиенте?».

– Конечно, – ответила Дженни. – Он повредил ваш компьютер? Это ужасно.

– Да.

«Чем я могу помочь?» – спросила Дженни.

Атакующий сообщил сведения, собранные во время тщательного поиска, чтобы подтвердить свою подлинность. Он узнал, что необходимые ему данные хранятся в информационной системе счетов клиентов (CBIS), и выяснил, как служащие обращаются к системе. Он спросил: «Вы можете посмотреть учетную запись в системе счетов?»

– Да, какой номер?

– У меня нет номера, мне нужно посмотреть по имени.

– Хорошо, какое имя?

«Хитер Марнинг» – он произнес имя по буквам, Дженни ввела его.

– О.К. Я нашла запись.

– Отлично. Запись действительна?

– Да, действительна

«Какой номер записи?»– спросил он.

– У вас есть карандаш?

– Я готов записывать.

– Номер записи BAZ6573NR27Q.

Он повторил номер и сказал: «Какой это адрес?»

Она сообщила ему адрес.

– Какой там телефон?

Дженни любезно зачитала ему и эти сведения.

Звонивший поблагодарил ее, попрощался и повесил трубку. Дженни продолжила работу со следующим звонком, никогда не вспоминая об этом.

Проект Арт Сили

Арт Сили отказался от работы свободного редактора, когда открыл, что мог заработать больше денег, делая исследования для писателей и коммерческих фирм. Он вскоре понял, что гонорар растет пропорционально тому, насколько близко требуется находиться к черте между законным и незаконным. Даже не осознавая этого, не называя это именем, Арт стал социальным инженером, применяя технологии, знакомые каждому информационному брокеру (information broker). У него оказался прирожденный талант к делу, он постиг методы, которым большинство социальных инженеров учатся у других. Спустя некоторое время он пересек черту без малейшего чувства вины.

Со мной связался человек, который писал книгу о кабинете министров в годы правления Никсона. Он искал того, кто мог бы найти сенсационную новость о Уильяме Саймоне (William E. Simon), министре финансов. Мистер Саймон умер, но автору было известно имя женщины, которая состояла в его штате. Он был уверен, что она жила в округе Колумбия, но не мог узнать адрес. Для ее имени не было указано телефона, или по

крайней мере не было среди перечисленных. Поэтому он позвонил мне. Конечно, нет проблем, сказал я ему.

Это работа, которую обычно можно выполнить с помощью одного или двух звонков, если вы знаете, что делаете. Можно считать, что каждая местная коммунальная компания выдает информацию за свои пределы. Конечно, вам придется немного наврать. Но что если немного невинной лжи сейчас, а потом – правда?

Мне нравится каждый раз применять различные подходы, так интереснее. «Это такой-то из исполнительных органов» всегда работало хорошо. «У меня на линии кто-то из из офиса вице-президента» сработало и в этот раз.

Сообщение от Митника

Никогда не думайте, что все атаки социальной инженерии нуждаются в тщательной разработке, такой сложной, что они могут быть опознаны до их окончания. Некоторые из них снаружи и изнутри, наступают и пропадают, очень простые атаки, которые не более чем… просьба.

Вам следует развить инстинкт социального инженера, чувствовать, насколько готов «сотрудничать» с вами человек на другом конце провода. В этот раз мне повезло с дружелюбной леди. С помощью одного телефонного звонка я узнал адрес и номер телефона. Миссия выполнена.

Анализ обмана

Конечно, Дженни знала, что информация о клиенте конфиденциальна. Она никогда не говорила об учетной записи одного клиента с другим клиентом и не распространяла частную информацию.

Но, естественно, для звонившего из компании применялись другие правила. В случае с сотрудником это рассматривалось как игра в команде и помощь друг другу в выполнении работы. Мужчина из отдела счетов мог бы сам уточнить подробности, если бы его компьютер не был выведен из строя вирусом, поэтому она была рада оказать помощь коллеге.

Арт постепенно добрался до ключевой информации, попутно задав вопросы о вещах, которые не были нужны на самом деле, таких как номер учетной записи. Тем не менее, номер учетной записи давал возможность отступления? если бы служащий стал подозревать что-либо, он позвонил бы второй раз, имея больше шансов на удачу, так как знание номера учетной записи внушало бы доверие следующему служащему.

С Джейн никогда так не обманывали в таких вещах, когда звонивший мог вообще не работать в отделе счетов. Конечно, здесь нет ее вины. Она не руководствовалась правилом, согласно которому надо убедиться в том, что вы знаете, с кем говорите, прежде чем сообщать сведения о клиенте. Никто не рассказал ей об опасности телефонных звонков, подобных тому, что сделал Арт. Этого не было в политике компании, это не

было частью ее обучения, и ее руководитель никогда не упоминал об этом.

Предотвращение обмана

В обучение безопасности следует включить следующий момент: звонящий или посетитель не является тем, за кого он себя выдает только потому, что он знает имена некоторых людей в компании или знает корпоративные терминологию или процессы. И это точно не доказывает, что он тот, кому разрешены выдача внутренней информации или доступ к компьютерной системе или сети.

Обучение безопасности должно подчеркивать: когда сомневаетесь, проверяйте, проверяйте, и еще раз проверяйте!

Раньше доступ к информации был признаком высокого положения и привилегии. Рабочие топили печи, запускали машины, печатали письма и сдавали отчеты. Мастер или начальник указывал, что, когда и как им делать. Мастер или начальник знал, сколько «штучек» (украшений) должен сделать работник за смену, сколько, каких цветов и размеров должна выпустить фабрик на этой неделе, на следующей, и к окончанию месяца.

Работники работали с машинами, инструментами и материалами, начальники работали с информацией. Работникам нужна была только специфическая информация, присущая их работе.

Сегодня немного другая картина, не так ли? Многие работники фабрик используют различные виды компьютеров и машин, управляемых компьютером. критическая информация на пользовательские компьютеры, чтобы они могли выполнить свою работу. В сегодняшних условиях почти все, чем занимаются служащие, связано с обработкой информации.

Вот почему политика безопасности компании должна распространяться по всему предприятию, независимо от положения служащих. Каждый должен понимать, что не только руководители, располагающие информацией, могут стать целью атакующего. Сегодня работники всех уровней, даже те, которые не используют компьютер, могут быть мишенью. Новые работники в группе обслуживания клиентов могут быть самым слабым звеном, которое социальный инженер использует для достижения своей цели. Обучение безопасности и корпоративная политика безопасности должны усилить это звено.

Глава 4: Внушая доверие

Перевод: (Теневой Георг, Whitewoolf@ukr.net, ICQ 118145).

Некоторые рассказы могли заставить Вас думать, будто я верю в то, что все на самом деле полные идиоты, готовые, даже жаждущие, отдать каждый секрет. Социальный инженер знает, что это неправда. Почему атака социальной инженерией так успешна? Это так, не потому что люди глупы или им не хватает здравого смысла… Просто мы, как люди, полностью уязвимы перед обманом, поскольку люди могут изменить доверие, если манипулировать определенным образом.

Социальный инженер ожидает подозрение и недоверие, и он всегда подготавливается, чтобы недоверие превратить в доверие. Хороший социальный инженер планирует атаку подобно шахматной игре, предполагая вопросы, которые цель атаки может задать, так что у него могут быть готовы подходящие ответы.

Одна из его основных техник включает создание чувства доверия со стороны его жертв. Как он заставляет Вас верить ему? Поверьте мне, может.

Доверие: ключ к обману

Чем естественней социальный инженер общается с жертвой, тем больше он ослабляет подозрение. Когда у людей нет причины для подозрений, социальному инженеру становится легко приобрести доверие жертвы.

Как только он получает ваше доверие, разводной мост опускается, и дверь замка распахивается, и он может зайти и взять ту информацию, что он хочет.

Заметка:

Вы можете заметить, как я ссылался на социальных инженеров, на телефонных фрикеров, и жуликов (con-game operators) в большинстве этих рассказов как «он». Это не – шовинизм; просто такова истина – большинство практикующий в этих областях – мужчины. Но, несмотря на это, среди социальных инженеров есть и женщины, число которых растет. Вы не должны терять бдительность и осторожность просто из-за того, что слышите женский голос. Фактически, женщины социальные инженеры имеют четкое преимущество из-за того, что они могут использовать свою сексуальность, чтобы получить сотрудничество. Вы найдете немножко так называемого слабого пола, представленного на этих страницах.

Первый звонок: Андреа Лопес

Андреа Лопес ответила на телефонный звонок в видео-прокате, где она работала, и сразу улыбнулась: всегда приятно, когда клиент говорит много хорошего про сервис. Тот, кто позвонил, сказал, что у него осталось очень хорошее впечатление о сервисе видео-проката, и он хотел послать менеджеру письмо, и сообщить об этом.

Он спросил имя менеджера и его почтовый адрес. Андреа сообщила ему, что менеджер это Томми Элисон, и дала адрес. Когда звонивший хотел положить трубку, у него появилась другая идея, и он сказал: «Я б мог написать в офис вашей компании, тоже. Какой номер вашего магазина?» Девушка также дала ему и эту информацию. Он поблагодарил, добавил что-то приятное про то, насколько полезной была она, и попрощался.

«Звонок подобный этому» – подумала Андреа, – «всегда помогает сделать карьерное продвижение быстрее. Как мило было бы, если люди делали подобное более часто».

Второй звонок: Джинни

«Спасибо за звонок в Видео Студию. Это – Джинни, чем могу Вам помочь?»

«Привет, Джинни», звонящий сказал с большим энтузиастом, как будто бы он говорил с Джинни каждую неделю или что-то вроде того.

"Это – Томми Элисон, менеджер магазин 863 в Фо-

рест Парке. У нас есть клиент здесь, что хочет арендовать *Рокки 5* , но у нас нет ни одного экземпляра. Вы можете проверить, есть ли у вас?"

Она вернулась на линию через несколько секунд и сказала: «Да, у нас есть три копии».

«Хорошо, я спрошу, хочет ли он подъехать к вам. Спасибо. Если Вам когда-либо будет нужна любая помощь нашего магазина, просто позвоните и попросите Томми. Я буду рад сделать для Вас все, что смогу».

Три или четыре раза на протяжении следующих нескольких недель, Джинни получала звонки от Томми для помощи в том или ином деле. Это были на вид законные просьбы, и он был всегда очень дружественным, не пытался сильно надавить. Он был очень болтливым, когда они общались, например – «Ты слышала о большом пожаре на Oak Park? Там, на перекрестке…», и тому подобное. Звонки были небольшим перерывом в рутине дня, и Джинни была всегда рада услышать его.

Однажды Томми позвонил и спросил: «У вас есть проблемы с компьютерами?»

«Нет» – ответила Джинни. «А почему должны быть?»

«Кто-то разбил автомобиль о телефонный столб, и телефонная компания заявляет, что целая часть города останется без связи и Интернета до тех пор, пока как они все исправят».

«О нет! Были человеческие жертвы?»

"Они увезли его в скорой помощи. Как бы то ни было, мне нужна небольшая помощь. Здесь ваш клиент, он хочет арендовать*Крестного Отца II* , и у него нет с собой его карты. Ты не могла бы проверить его информацию для меня?"

«Да, конечно».

Томми дал имя клиента и адрес, и Джинни нашла его в компьютере. Она дала Томми учетный номер.

«Никаких поздних возвращений или долга?» – Спросил Томми.

«Ничего не вижу»

«Хорошо, прекрасно. Я подпишу его вручную для счета и внесу в нашу базу данных позже, когда компьютеры снова заработают нормально. Он хочет оплатить счет карточкой Visa, которую он использует в вашем магазине, а у него нет с собой карты. Какой номер карты и дата истечения срока?»

Она дала ему номер, вместе с датой истечения срока. Томми сказал: "Спасибо за помощь. Поговорим позже”, и положил трубку.

История Долли Лоннеган.

Лоннеган – это не тот молодой человек, которого вы хотели бы увидеть, когда открываете входную дверь. Бывший сборщик долгов в азартных играх, он все еще делает это иногда. В этом случае, ему предлагали значительную суму наличных за несколько телефонных

звонков в видеомагазин. Звучит достаточно просто. Никто из этих «клиентов» не знал, как проделать этот трюк; им нужен кто-то с талантом Лонеганна.

Люди не выписывают чеки, чтобы покрыть их долги, когда им не везет или они поступают глупо за игрой в покер. Каждый знает это. Почему эти старые друзья продолжали играть с жуликом, что не имел денег на столе? Не спрашивайте. Может быть, у них чуть-чуть меньше IQ, чем у остальных. Но они – старые друзья – что вы можете поделать?

Этот парень не имел денег, так что они взяли чек. Я спрашиваю вас! Надо было бы подвести его к машине ATM(аппарат обналички чеков?), – вот что надо было сделать. Но нет, чек. На $3,230.

Естественно, он обманул. Чего вы еще ожидали? Потом они позвонили мне; могу ли я помочь? Я не закрываю двери перед людьми, которые пришли ко мне. Кроме того, в настоящее время есть лучшие пути. Я сказал им, что 30 процентов комиссионных мои, и я посмотрю, что смогу сделать. Итак, они дали мне его имя, адрес и я нашел в компьютере ближайший к нему видео магазин.

Я не очень спешил. Четыре телефонных звонка к менеджеру магазина, и затем, бинго – у меня есть номер карты Visa мошенника.

Другой мой друг – хозяин topless бара. За пятьдесят долларов, он сделал проигранную парнем сумму де-

нег в покер долгом бару (через Visa). Пускай мошенник объясняет это все своей жене. Вы думаете, он мог бы попытаться сообщить в Visa, что это не его долг? Подумайте снова. Он знает, что нам известно кто он. И если мы смогли получить его номер карточки Visa, он догадается, что мы можем получить намного больше. Не волнуйтесь на этот счет.

Анализ обмана

Звонки Томми к Джинни были просто для построения доверия. Когда время пришло для атаки, она потеряла бдительность и осторожность и сообщила Томми о том, про кого он спросил, так как он – менеджер в другом магазине одной компании.

И почему она помогла ему – она уже знала его. Она только познакомилась с ним через телефон, но они установили деловую дружбу, которая является основой для доверия. Однажды она приняла его как менеджера в той же компании, доверие было установлено, а остальное было уже как прогулка в парке.

Сообщение от Митника

Техника построения доверия является одной из наиболее эффективных тактик социальной инженерии. Вы должны подумать, хорошо ли вы знаете человека, с которым вы говорите. В некоторых редких случаях, человек может быть не тем, кем он представился. Следовательно, мы должны научиться наблюдать, думать, и спрашивать о полномочиях.

Вариации по теме: Сбор кредитных карт

Строя доверие не обязательно требуется делать целую серию звонков, как в предыдущей истории. Я расскажу один случай, где мне потребовалось всего пять минут.

Сюрприз для Папы

Я один раз сидел за столом в ресторане с Генри и его отцом. В ходе разговора, Генри упрекал отца в раздаче номера его кредитной карточки как если бы, это был его номер телефона. «Конечно, ты должен дать номер карты, когда ты покупаешь что-то», он сказал. «Но давать номер карточки в магазине, что записывает номер – это действительно глупо».

«Единственное место, где я сделал это, была Видео Студия», – сказал мистер Конклин, назвав ту самую сеть видео магазинов. "Но я проверяю мои счета в Visa каждый месяц. Если расходы будут превышать ожидаемое, я узнаю об этом.

“Уверен", сказал Генри, «но как только у них появится твой номер, очень легко можно будет его украсть».

“Ты имеешь в виду плохого служащего”?

“Нет, *кто-нибудь* – не обязательно служащий".

“Ты говоришь глупости," сказал мистер Конклин.

“Я могу позвонить прямо сейчас и заставить их, чтобы сообщили мне твой номер карточки Visa," – не успокоился Генри.

“Нет, ты *не сможешь* ” – ответил отец.

«Я могу сделать это прямо перед тобой за 5 минут, не покидая стола».

Мистер Конклин огляделся, со взглядом того, кто чувствует уверенность в себе, но не хочет показывать это. «Я говорю что ты не знаешь, что говоришь», – гаркнул он, вытаскивая бумажник и ложа пятьдесят долларов на столе. "Если ты сможешь сделать то, про что ты говоришь, то это твое”.

«Мне не нужно твоих денег, папа», —сказал Генри.

Он вытащил сотовый телефон, спросил отца, каким филиалом он пользуется, и позвонил помощнику директора также как и на номер магазина в соседнем Sherman Oaks.

Затем он позвонил в магазин на Sherman Oaks. Используя тот же метод, что описывался в предшествующем рассказе, он быстро узнал имя менеджера и номер магазина.

Затем он позвонил в магазин, где у его отца был счет. Он использовал старый трюк с менеджером, используя имя менеджера как его собственное и номер магазина, который он только что получил. Потом использовал ту же уловку:

«Ваши компьютеры работают хорошо? Наши сильно

заглючили».

Он услышал ответ менеджера и затем сказал: «Хорошо, у меня здесь один из ваших клиентов, который хочет арендовать видео, но наши компьютеры сейчас не работают. Мне нужно чтобы вы нашли счет клиента и убедились что он – клиент вашего филиала».

Генри дал ему имя отца. Затем, использовав только легкое изменение в технике, он попросил прочитать информацию о счете: адрес, номер телефона, и дату когда счет был открыт. И затем он сказал, «Слушайте, у меня тут большая очередь клиентов. Какой номер кредитной карточки и дата истечения срока?»

Генри прижал телефон одной рукой к уху, пока он писал на бумажной салфетке другой рукой. Когда разговор был завершен, он положил салфетку перед его отцом, который пристально наблюдал за этим с открытым ртом. Мистер Конклин выглядел полностью потрясенным, как если бы его доверие только что рухнуло.

Анализ обмана

Думайте что говорите, когда кто-то неизвестный вам спрашивает о чем-то. Если грязный незнакомец постучит в вашу дверь, вы вряд ли позволите ему войти, а если незнакомец постучит в вашу дверь хорошо одетый, с начищенными до блеска туфлями, хорошей прической, с хорошими манерами и улыбкой, Вы, вероятно, будете значительно меньше подозрительными. Может быть он – действительно Джейсон из фильма *Пят-*

ница 13-е , но вы начинаете ему доверять, пока он нормально выглядит и без ножа в руке.

Что менее очевидно – то, что мы судим людей по телефону точно так же, как и обычно. Говорит ли этот человек так, как будто пытается продать мне что-то? Он дружелюбный и общительный или я чувствую враждебность или давление? Говорит ли он или она как образованный человек? Мы судим по этим вещам и возможно, многим другим бессознательно, в спешке, часто во время первых секунд разговора.

Сообщение от Митника

Человеку свойственно думать, что вряд ли его обманут именно в этой конкретной сделке, по крайней мере, пока нет причин предполагать обратное. Мы взвешиваем риски и затем, в большинстве случаев, доверяем без всяких сомнений. Это естественное поведение цивилизованного человека… по крайней мере, цивилизованных людей, которыми никогда не манипулировали или не обманывали на крупную суму денег.

Когда мы были детьми, наши родители учили нас не верить незнакомцам. Может быть, нам всем следовало бы придерживаться этому вековому принципу в сегодняшней рабочей обстановке.

В работе, люди просят нас все время о чем-то. Вы имеете электронный адрес этого парня? Где самая последняя версия списка клиентов? Кто субподрядчик в этой части проекта? Пожалуйста, пошлите мне самое

последнее обновление проекта. Мне нужна новая версия исходного кода.

И как можно догадаться: иногда люди, которые просят о чем-либо, являются людьми, которых вы не знаете лично, к примеру, те, кто работает в другой части компании. Но если информация, которую они дают, подтверждается, и, оказывается, что они знакомы («Марианна сказала…»; «Это находится на сервере К-16…»; «… исправленное издание 26 нового продукта планируется»), мы расширяем наш круг доверия, чтобы включить их, и радостно даем им то, о чем они просят.

Конечно, мы не всегда спрашиваем себя: «Почему кому-то на заводе в Далласе нужно увидеть новые планы продукта?» или « могло бы навредить чему-нибудь, если дать имя сервера, где они находятся?» Итак, мы задаем иные вопросы. Если ответы являются разумными и произносятся в нормальном тоне, мы понижаем бдительность, возвращаясь к нашей естественной склонности доверять нашему «приятелю» мужчине или женщине, и сделаем (в рамках разумного) все, что нас попросят сделать.

И не думайте, что нападающий атакует только тех людей, которые пользуются компьютерной системой компании. Как насчет парня в почтовой комнате? «Вы хотите меня о чем-то попросить? Бросить это во внутренний почтовый ящик компании?» Клерк из комна-

ты почты знает, что там дискетка со специальной небольшой программой для секретаря CEO, управляющего делами? Теперь нападающий получает собственную персональную копию email CEO. ОПА! Могло ли что-то подобное случаться в вашей компании? Ответ – конечно.

Одноцентовый сотовый телефон

Многие люди оглядываются пока не найдут лучшую сделку; социальные инженеры не ищут лучшую сделку, они ищут путь, чтобы сделать сделку выгоднее. Например, иногда компания запускает маркетинговую кампанию, так что вы не можете пропустить ее, пока социальный инженер смотрит на предложение и гадает, как он может улучшить сделку.

Недавно, у национальной сотовой компании была акция: предлагали новый телефон за один цент, если вы подпишете контракт.

Очень много людей обнаружило слишком поздно, что есть много вопросов, которые предусмотрительный покупатель должен спрашивать прежде, чем подписаться на контракт сотовой связи: план услуг аналоговый, цифровой, или комбинированный; количество бесплатных минут в месяц; включена ли в цену плата за роуминг, и так далее. Особенно важно, чтобы понять перед заключением контракта, на сколько месяцев или лет Вы заключаете контракт?

Одного социального инженера в Филадельфии привлек дешевый телефон, предложенный сотовой компанией в контракте, но он ненавидел тарифные планы, которые были в контракте. Не проблема. Вот один

путь, по которому он мог управлять ситуацией.

Первый звонок: Тед

Сначала, социальный инженер звонит в магазин электроники в West Girard.

«Электронный Город. Это Тед.»

"Привет, Тед. Это – Адам. Слушай, Я пару дней назад говорил с продавцом о сотовом телефоне. Я сказал ему что перезвоню, когда решу, какой тарифный план выбрать, и я забыл его имя. Кто тот парень, который работал в этом отделе на днях?

«Тут не один продавец. Это был Вильям?»

«Я не уверен. Может быть, это было Вильям. Как он выглядит?» «Высокий худой парень».

«Я думаю, это был он. Повторите пожалуйста, как его фамилия?»

«Хедли Х—Е—Д—Л—И»

«Да, вроде это был он. Когда он снова будет?»

Я не знаю его расписание на эту неделю, но на вторую смену люди приходят около пяти".

«Хорошо. Я проговорю с ним сегодня вечером. Спасибо, Тед.»

Второй Звонок: Кети

Следующий звонок – в магазин той же самой компании на North Broad Street.

«Привет, Электронный Город. Кети на проводе, чем могу вам помочь?»

«Кети, Привет. Это – Вильям Хедли, из магазина на

West Girard. Как идут сегодня дела?»

«Неважно, а что случилось»

«У меня есть клиент, который пришел по акции “сотовый телефон за один цент”. Знаешь что я имею в виду?»

«Знаю. Я продала пару таких на прошлой неделе».

«У вас еще есть телефоны, которые идут с этой акцией?»

«Получили кучу таких».

«Прекрасно. Я только что продал один клиенту. Парень заплатил кредит; мы подписали с ним контракт. Телефон оказался бракованным, и у нас больше нет ни одного телефона. Я так смущен. Вы можете мне помочь? Я пошлю его в ваш магазин, чтобы приобрести телефон. Вы можете продать ему телефон за один цент? И он обязан перезвонить мне, как только он получит телефон, чтобы я смог ему рассказать про акцию».

«Да, конечно. Пришлите его сюда».

«Хорошо. Его имя Тед. Тед Янеси.»

Когда парень, который назвал себя Тедом Янеси, появился в магазине на улице North Broad St. Кети выписала счет и продала сотовый телефон за один цент, так как ее просил коллега. Она попалась на трюк мошенника.

Когда пришло время заплатить, покупатель не имел ни цента в кармане, так что он добрался до небольшой

тарелки с мелочью у кассового аппарата, взял один, и дал девушке за регистрацию. Он получил телефон, не платя ни одного цента за это.

Теперь он может прийти в другую компанию, которая использует телефоны того же стандарта и заказать себе другой тарифный план без контрактных обязательств.

Анализ обмана

Людям естественно доверять в более высокой степени коллеге, который что-то просит, и знает процедуры компании, жаргон. Социальный инженер в этом рассказе воспользовался преимуществом, узнав детали компании, выдавая себя за служащего компании, и прося помощи в другом филиале. Это случается между филиалами магазинов и между отделами в компании, люди физически разделяются и общаются по телефону, никогда не встречая друг друга.

Взлом федералов

Люди часто не думают, какие материалы их организации доступны через Интернет. Для моего еженедельного шоу на KFI Talk Radio, в Лос-Анджелесе продюсер покопался в сети и обнаружил копию руководства для получения доступа к базам данных Национального Центра Информационных Преступлений. Позже он обнаруживал реально работающее руководство NCIC, секретный документ, который дает возможность для поиска информации из национальной базы данных FBI.

Руководство является справочником для агентств силовых ведомств, который дает коды для поиска информации о преступниках и преступлениях из национальной базы данных. Агентства всей страны могут найти ту же базу данных для информации, для помощи, в борьбе с преступностью в своей юрисдикции. Руководство содержит коды, использованные в базе данных начиная с татуировок, заканчивая маркировкой украденных денег и обязательств.

Любой с доступом к руководству может найти синтаксис и команды, чтобы получить информацию из национальной базы данных. Затем, следуя инструкциям из руководства, каждый может извлечь информацию

из базы данных. Руководство также дает телефонные номера технической поддержки в системы. Вы можете иметь аналогичные описания в вашей компании, предлагающей коды продуктов или коды для доступа к важной секретной информации.

Несомненно, ФБР бы никогда не обнаружило, что их важнейшие руководства и инструкции доступны для каждого в сети, и я не думаю, что они были бы очень счастливы, узнав об этом. Одна копия была опубликована государственным отделом в Орегоне, другая правоохранительными органами в Техасе. Почему? В каждом случае, они, вероятно, подумали, что информация не была важна и, став доступной, она не могла причинить вред. Может быть, кто-то поместил это в их внутренней сети для удобства собственным служащим, иногда не понимая, что информация стала доступна для любого в Интернет, кто имеет доступ к хорошей поисковой машине, как, например, Google – включая просто любопытных, продажных полицейский, хакеров, и преступные организации.

Подключение к системе

Принцип использования такой информации для обмана кого-то в государственной или коммерческой организации тот же: поскольку социальный инженер знает, как получить доступ к специальным базам данных или приложениям, или узнать имена серверов компании, жертвы начинают полагать, что он говорит правду.

И это ведет к доверию.

Если социального инженера есть такие коды, то получение информации для него – легкий процесс. В этом примере, он мог начать со звонка служащему местного полицейского управления, и задать вопросы относительно одного из кодов в руководстве – например, код правонарушения. Он мог, например, говорить «когда я делаю запрос в NCIC, я получаю ошибку „Системная ошибка“. Вы получаете то же самое, делая запрос? Вы не могли бы пробовать это для меня?» Или он может сказать, что попытался найти *wpf* – на полицейском жаргоне файл на разыскиваемую особу.

Служащий на другом конце телефона узнает по жаргону, что звонящий знаком с процедурами и командами запросов в базе данных NCIC. Кто еще кроме служащих может знать такие тонкости?

После того, как служащий подтвердит, что система работает хорошо, разговор мог быть приблизительно таким:

«Я мог бы вам немножко помочь. Что Вы ищете»?

«Мне нужно сделать запрос про Редрона, Мартина. Дата рождения 10/18/66.»

«Что какой у него SOSH?» (Служители закона иногда ссылаются на номер социального страхования как *SOSH* .)

«700-14-7435.»

После просмотра листинга, он могла бы сказать, на-

пример, «Его номер – 2602.»

Атакующий должен только посмотреть в базе NCIC, чтобы узнать значение числа: какие преступления совершил человек.

Анализ обмана

Совершенный социальный инженер не остановится ни на минуту, чтобы обдумывать пути взлома базы данных NCIC. А зачем задумываться, когда он просто позвонил в местный полицейский отдел, спокойно говорил, и звучал убедительно, будто он работает в компании, – и это все, что потребовалось, чтобы получить нужную ему информацию? И в следующий раз, он просто позвонит в другой полицейский участок и использует тот же предлог.

LINGO

SOSH – сленг правоохранительных органов для номера социального страхования.

Вы могли удивиться, не рискованно ли позвонить полицейский участок, офис шерифа, или в офис дорожного патруля? Не сильно ли атакующий рискует?

Ответ – нет… и по особой причине. Служители закона, подобно военным, имеют укоренившееся в них из первого дня в академии отношение к высшим или низшим по званию (рангу). Пока социальный инженер выдает себя сержантом или лейтенантом – т.е человеком с более высоким званием, чем тот, с кем он общается – жертвой будет управлять этот хорошо запомненный

урок, который говорит, что вы не должны задавать вопросы людям, что выше вас званием. Звание, другими словами, имеет привилегии над теми, у кого более низкий чин.

Но не думайте что полицейские участки и военные структуры – единственные места, где социальный инженер может использовать привилегии в звании. Социальные инженеры часто используют «преимущество высокого ранга» в корпоративной иерархии как оружие в атаке на предприятиях – что демонстрируются во многих рассказах в этой книге.

Предотвращение обмана

Какими мерами может воспользоваться ваша организация, чтобы уменьшить вероятность, что социальные инженеры воспользуются преимуществом над природными инстинктами ваших служащих, чтобы поверить людям? Вот некоторые меры.

Защитите ваших клиентов

В наш электронный век многие компании, продающие что-то потребителю, сохраняют кредитные карты в файле. На то есть причины: он облегчает клиенту работу, обеспечивая информацией о кредитной карточке всякий раз, когда он посещает магазин или веб-сайт, чтобы оплатить. Тем не менее, практика огорчает.

Если Вам приходится сохранять номера кредитных карточек в файле, то это должно сопровождаться мерами безопасности, которые включают шифрование или использование управления доступом. Служащие должны быть подготовленными, чтобы распознать трюки социальных инженеров, как в этой главе. Служащий компании, которого вы никогда лично не видели, ставший телефонным другом, может быть не тем, за кого он себя выдает. Ему необязательно знать, как получить доступ к секретной информации клиента, потому что он может вовсе не работать в вашей компании.

Сообщение от Митника

Все должны быть осведомлены о методах действия социальных инженеров: собрать как можно больше информации о цели, и использовать, эту информацию, чтобы приобрести доверие как будто он свой человек. А затем перейти в нападение!

Разумное доверие

Не только люди, имеющие доступ к важной информации – разработчики программного обеспечения, сотрудники в научно-исследовательских и опытно-конструкторских работ, должны быть защищены от атаки. Почти каждый в вашей организации должен быть обучен защищать предприятие от промышленных шпионов и похитителей информации.

Создавая основы, нужно начать с обследования предприятия – доступ к банкам информации, уделяя внимание каждому важному, критическому аспекту, ценным активам, и спрашивая, какие методы нападения могут использовать, чтобы с помощью техники социальной инженерии получить доступ к этим ценным данным. Соответственная подготовка для людей, которые имеют доступ к такой информации, должна проектироваться вокруг ответов на эти вопросы.

Когда кто-то незнакомый вам лично просит некоторую информацию или материал, или просит, чтобы вы выполнили любые команды на вашем компьютере, нужно задать себе следующие вопросы. Если я дал эту

информацию моему наихудшему врагу, могло бы это использоваться, чтобы повредить мне или моей компании? Я полностью понимаю потенциальный результат команд, что меня попросили ввести в компьютер?

Мы не хотим прожить жизнь, подозревая каждого нового человека, которого мы встречаем. Но чем больше мы доверчивы, тем больше вероятность того, что следующий социальный инженер, который появился в городе, сможет обмануть нас, заставить выдать конфиденциальную информацию нашей компании.

Что принадлежит к вашей внутренней сети?

Части вашей внутренней сети могут быть открытыми для всего мира, а другие части – только для ограниченного числа сотрудников. Насколько ваша компания убеждена, что важнейшая информации не опубликована там, где она доступна для пользователей, от которых вы хотите защитить ее? Когда в последний раз кто-нибудь в вашей организации проверял, доступна ли важная информация из вашей внутренней сети? Что доступно через открытые части вашего веб-сайта?

Если ваша компания установила прокси-серверы как посредники, чтобы защитить предприятие от электронной атаки, проверены ли эти серверы, чтобы убедиться, что они сконфигурированы правильно?

И вообще, проверял ли когда-либо кто-либо безопасность вашей внутренней сети?

Глава 5: «Разрешите Вам помочь»

Перевод: Daughter of the Night (admin@mitnick.com.ru)

Мы все благодарны, когда кто-нибудь со знанием, опытом и желанием помочь приходит и предлагает помочь с проблемами. Социальный инженер понимает это, и знает, как извлечь из этого выгоду.

Он также знает как *создать* вам проблему… а потом сделать вас благодарными, когда он решит проблему… и на вашей поиграв на вашем чувстве благодарности, извлечет из вас информацию или попросит оказать небольшую услугу, которая оставит вашу компанию (или вас лично) в гораздо более плохом состоянии после встречи. И вы можете даже не узнать, что вы потеряли что-то ценное.

Есть несколько типичных способов, которыми социальные инженеры пытаются «помочь».

Неполадки в сети

Дата/Время: Понедельник, 12 февраля, 15:25

Место: Офис кораблестроительной фирмы Starboard.

Первый звонок: Том ДиЛэй

«Том ДиЛэй, бухгалтерия».

«Здравствуй, Том, это Эдди Мартин, отдел техпомощи, мы пытаемся найти причины неисправности компьютерной сети. Были ли у кого-либо в вашей группе проблемы с подключением?»

«Нет, я не в курсе».

«А у тебя?»

«Нет, все вроде в порядке».

«Окей, это хорошо. Мы звоним людям, на кого это может повлиять, потому что важно всех проинформировать заранее, если будут внезапные отключения».

«Это звучит нехорошо. Вы думаете, это может случиться?»

«Надеюсь, что нет, но если что случится, позвонишь?»

«Можешь не сомневаться».

«Похоже, отсутствие связи будет для тебя проблемой».

"*Бесспорно* ".

«Так что пока мы над этим работаем, я дам тебе свой сотовый. Тогда ты сможешь мне все сообщить при первой необходимости».

«Отлично, говори».

«Номер 555 867 5309».

«555 867 5309. Записал. Спасибо. А как тебя зовут?»

"Эдди. И последнее. Мне надо знать, к какому порту подключен твой компьютер. Посмотри, там где-то есть наклейка с надписью «Порт N…»

«Сейчас… Нет, не вижу ничего подобного».

«Ладно, тогда сзади компьютера. Ты узнаешь сетевой провод?»

«Да».

«Тогда посмотри, где он подключен. Там должна быть табличка».

«Подожди секунду. Сейчас. Мне придется туда пролезть, чтобы ее увидеть. Вот. На ней написано Порт 6-47.»

«Отлично, как раз как записано про тебя. Просто проверяю».

Второй звонок: Человек из техобслуживания

Через пару дней поступил звонок в отдел локальной сети.

«Здравствуй, это Боб, я в офисе Тома ДиЛэя из бухгалтерии. Мы пытаемся найти неисправность в кабеле. Надо отключить порт 6-47.»

Человек из техобслуживания сказал, что это будет

сделано за несколько минут, и попросил перезвонить, когда потребуется включить порт.

Третий звонок: Помощь от врага.

Примерно через час, человек, представившийся как Эдди Мартин, ходил по магазинам в Circuit City, и вдруг зазвенел телефон. Он посмотрел номер звонящего, узнал, что он из кораблестроительной компании поспешил в спокойное, тихое место, прежде чем ответить.

«Отдел техпомощи, Эдди.»

«О, здравствуй, Эдди. Проблемы со связью. Ты где»?

«Я, э, в кабельной комнате. Кто это»?

«Это Том ДиЛэй. Я рад, что нашел тебя. Может, помнишь, ты мне звонил недавно? Мое соединение не работает, как ты и говорил, и я немножко паникую».

«Да, у нас сейчас отключена куча людей. Но мы все поправим к концу дня. Сойдет»?

«НЕТ! Черт, я серьезно отстану, если я буду отключен столько времени. Никак нельзя побыстрее»?

«Насколько это важно?»

«Пока я могу заняться другими делами. Может, ты все поправишь за полчаса?»

«ПОЛЧАСА? Ну ладно, я брошу то, чем я занимаюсь, и попытаюсь сделать что-нибудь для тебя».

«Я очень благодарен, Эдди!»

Четвертый звонок: Попался!

Через 45 минут…

«Том? Это Эдди. Проверь свое подключение».

Через несколько минут:

«Отлично, оно работает. Великолепно».

«Хорошо, что я смог тебе помочь».

«Да, спасибо большое».

«Слушай, если ты хочешь быть уверен, что твое подключение больше не прервется, надо поставить одну программку».

«Сейчас не лучшее время».

«Я понимаю… Но зато не будет проблем в следующий раз, когда произойдет сбой сети».

«Ну… только если это займет несколько минут».

«Вот что надо сделать…»

Эдди рассказал Тому, как скачать маленькое приложение с одного сайта. После того, как программа скачалась, Эдди сказал запустить ее двойным щелчком мыши. Он попробовал и сказал:

«Не работает. Она ничего не делает».

«Ужас. Наверно, что-то не так с программой. Давай от нее избавимся, и попробуем еще раз в другое время». Он рассказал Тому, как безвозвратно удалить программу.

Затрачено времени: 12 минут.

История атакующего

Бобби Уоллас считал, что это смешно, когда он находил хорошее задание, вроде этого, и его клиент увиливал от неприкрытого, но очевидного вопроса – за-

чем ему нужна эта информация. В данном случае он мог предположить, что могут быть только две причины. Возможно, они были заинтересованы в покупке кораблестроительной компании Starboard, и хотели узнать, как у них обстоят дела с финансами – особенно все то, что компания может скрывать от потенциального покупателя. Или они были представителями инвесторов, которые думали, что есть что-то подозрительное в том, что делается с деньгами, и хотели узнать, не вмешаны ли их исполнители во что-либо.

А возможно, клиент не хотел говорить Бобби истинную причину потому, что если он узнает, насколько ценна информация, он, скорее всего, попросит больше денег.

Существует множество способов взломать самые секретные файлы компании. Бобби провел несколько дней, обдумывая различные варианты и выполняя небольшую проверку перед тем, как он наметил план. Он остановился на том, в котором применялся его любимый подход, где все подстроено так, что жертва просит атакующего о помощи.

Для начала, Бобби купил сотовый телефон за $39.95 в продуктовом магазине. Он позвонил мужчине, которого он выбрал в качестве цели, представился сотрудником техподдержки компании, и устроил все так, чтобы мужчина позвонил Бобби на сотовый, если возникнет проблема с сетью.

Он сделал паузу в несколько дней, чтобы все не было слишком очевидно, и позвонил в центр сетевых операций (network operations center, NOC) той компании. Он утверждал, что устраняет проблему для Тома, его жертвы, и попросил отключить сеть Тому. Бобби знал, что это была самая коварная часть плана – во многих компаниях люди из техпомощи тесно общались с NOC; на самом деле, он знал, что техпомощь обычно является частью IT отдела организации. Но равнодушный парень из NOC, с которым он говорил, принял звонок как рутину, и даже не спросил имя человека из техпомощи, который теоретически работал над проблемой в сети, и согласился отключить сетевой порт «цели». Когда все будет сделано, Том будет полностью изолирован от локальной сети компании, не сможет работать с файлами с сервера, обмениваться информацией с сотрудниками, скачивать почту, и даже отправлять страницы на принтер. В сегодняшнем мире, это все равно, что жить в пещере.

Как Бобби и ожидал, вскоре зазвенел его сотовый. Конечно, он старался звучать так, будто он жаждет помочь своему «товарищу-сотруднику» в беде. Тогда он позвонил в NOC и вновь включил сетевое соединение мужчины. Наконец, он позвонил мужчине и снова использовал его, на этот раз, заставив его почувствовать вину, сказав «нет» после того, как Бобби оказал ему услугу. Том согласился выполнить просьбу и скачал

программу на свой компьютер.

Конечно, то, с чем он согласился, не было тем же, чем казалось. Программа, которая, как было сказано Тому, должна была предотвращать отключение его соединения, на самом деле была *троянским конем* – программным приложением, которое сделало с компьютером Тома то же, что первоначально сделали с Троянцами: она была внесена противником в лагерь. Том отчитался, что ничего не произошло, когда он 2 раза кликнул по ярлыку; на самом деле, было задумано, чтобы он не мог видеть, как что-то происходит, даже не смотря на то, что приложение установило секретную программу, которая позволит взломщику получать скрытый доступ к компьютеру Тома.

С работающей программой, Бобби получал полный контроль над компьютером Тома, который называется удаленной *командной строкой* . Когда Бобби подключился к ПК Тома, он смог посмотреть все бухгалтерские файлы, которые могут оказаться интересными, и скопировать их. Затем, в свое удовольствие, он проверил файлы на наличие информации, которая даст клиентам то, чего они ищут.

LINGO

Троянский конь – программа, содержащая хулиганский или вредоносный код, созданная для того, чтобы повредить компьютер или файлы жертвы, или получить данные из компьютера или сети. Некоторые тро-

яны прячутся в ОС компьютера, и смотрят за каждой нажатой клавишей или действием, или принимают команды через сетевое соединение с целью выполнения некоторой функции, и это происходит без ведома жертвы.

И это было еще не все. Он мог вернуться в любое время, и просмотреть электронную почту и личные памятки служащих компании, сделав поиск текста, который сможет показать любые лакомые кусочки информации.

Поздно, тем же вечером, когда он обманом заставил свою жертву установить троянского коня, Бобби выкинул свой сотовый в помойку. Конечно, он был осторожен, и очистил память, а потом вытащил батарейку, прежде чем выбросить его – ему меньше всего было надо, чтобы кто-нибудь случайно набрал номер, и телефон зазвонил.

Анализ обмана

Атакующий плетет сети для того, чтобы убедить жертву, что у него есть проблема, которая на самом деле не существует. Или, как в данном случае, проблема, которой пока нет, но атакующий знает, что она *будет* , так как он ее и создаст. Он представил себя человеком, способным найти решение.

Организация этого вида атаки особенно привлекательна для атакующего. Из-за того, что все было спланировано заранее, когда «цель» узнает, что у него есть

проблема, он звонит и умоляет о помощи. Атакующий просто сидит и ждет, когда зазвенит телефон – эта тактика более известна, как *обратная социальная инженерия* . Атакующий, который может заставить жертву позвонить *ему* , получает мгновенное доверие: «если я позвоню кому-нибудь, кто, как мне кажется, из технической поддержки, я не буду просить его подтвердить свою личность». В этот момент можно считать, что атакующий уже победил.

LINGO

Удаленная командная строка – Неграфический интерфейс, который принимает текстовые команды для выполнения определенных функций или запуска программ. Атакующий, который эксплуатирует технические уязвимости или может установить Троянского Коня на компьютер жертвы, получает доступ к удаленной командной строке.

Обратная социальная инженерия – Социально инженерная атака, в которой атакующий создает ситуацию, где жертва сталкивается с проблемой, и просит атакующего о помощи. Другая форма обратной социальной инженерии переводит стрелки на атакующего. Цель распознает атаку и использует психологические приемы, чтобы узнать как можно больше информации об атакующем, чтобы бизнес мог направленно охранять свое имущество.

Сообщение от Митника

Если незнакомый человек окажет вам услугу, а потом попросит сделать что-либо, не делайте этого, не обдумав хорошенько то, что он просит.

В афере, подобной этой, социнжинер пытается выбрать такую цель, у которой ограниченные знания в области использования компьютеров. Чем больше он знает, тем больше вероятность того, что он что-то заподозрит, или поймет, что его пытаются использовать. Такой человек, который мало знает о технике и процедурах, «рабочий, бросивший вызов компьютеру», скорее всего, подчинится. Очень вероятно, что он попадет на уловку вроде «Просто скачайте эту программу», потому что даже не подозревает, сколько вреда может принести подобное ПО. Помимо этого, зачастую он не понимает ценности информации, которой он рискует.

Немного помощи для новенькой девушки.

Новые сотрудники – сочные цели для атакующих. Они еще многого не знают – они не знают процедуры, что можно и что нельзя делать в компании. И, ради создания хорошего впечатления, они жаждут показать, как быстро и хорошо они могут работать и откликаться на просьбы.

Доброжелательная Андреа

«Отдел кадров, говорит Андреа Калхун».

«Андреа! Привет, это Алекс, отдел безопасности корпорации».

«Да».

«Как твои дела сегодня»?

«Все ОК, чем могу быть полезна?»

«Слушай, мы тут планируем семинар по безопасности для новых сотрудников, надо подыскать несколько человек. Мне нужен список имен и телефонов сотрудников, которых взяли на работу за последний месяц. Можешь мне с этим помочь?»

«Но я не смогу сделать это до обеда, это не страшно? В каком отделении ты работаешь?»

"А, ладно, отделение 52… но я буду почти весь день на деловых встречах. Я тебе перезвоню, когда буду в

офисе, где-то после 4-х.

Когда Алекс позвонил где-то в 4:30, Андреа уже подготовила список и прочла ему имена и номера отделений.

Сообщение для Розмери

Розмери Морган была очень рада получить эту работу. Она никогда раньше не работала в издательстве, и все казались ей гораздо более дружелюбными, чем она ожидала, что удивительно, учитывая бесконечное напряжение под которым находился коллектив, чтобы успеть сделать новый номер за месяц. И звонок в этот четверг подтвердил ее впечатление о дружелюбии.

«Вы Розмери Морган?»

«Да»

«Здравствуй, Розмери, это Билл Джордай, отдел безопасности информации».

«Чем могу быть полезна»?

«Кто-нибудь из нашего отдела обсуждал с тобой технику безопасности?»

«Вроде, нет».

«Так, посмотрим. Для начала, мы не позволяем никому устанавливать программное обеспечение не из компании. Это потому что мы не хотим отвечать за использование лицензионных программ. А также чтобы избежать проблем с программами, содержащими червь или вирус».

«Окей.»

«А ты знаешь, что мы предпринимаем для безопасности электронной почты?»

«Нет».

«Какой у тебя сейчас e-mail»?

"**Rosemary@ttrzine.net** "

«Вы используете логин Rosemary»?

"Нет, *RMorgan"* .

«Итак. Всем новым сотрудникам надо знать, что опасно открывать вложенные файлы, которых вы не ожидаете… Много вирусов и червей распространяются и приходят ос адресов тех людей, кого вы знаете. Так что если ты не ожидала письма с вложением, ты должна проверить, действительно ли отправитель его отправил. Понятно?»

«Да, я об этом слышала».

«Отлично. По нашим требованиям, пароль надо менять каждые 90 дней. Когда ты в последний раз меняла пароль?»

«Я тут всего две недели, и использую тот, который я в начале поставила».

«Окей. Это хорошо. Но мы должны быть уверены, что люди используют пароли, которые не слишком легко отгадать. Используешь ли ты пароль, состоящий из букв и цифр?»

«Нет».

«Ну, мы это поправим… Какой пароль ты используешь сейчас?»

«Имя моей дочери – Annette.»

«Это не очень безопасный пароль. Ты никогда не должна использовать пароль, основанный на семейной информации. Так, посмотрим. Вы можете сделать так же, как я. То, что ты используешь сейчас, сойдет для 1-й части пароля, но каждый раз, когда его меняешь, добавляй число текущего месяца».

«Так что если я сменю пароль сейчас, в Марте, я поставлю „3“».

«Это уже как хочешь. Какой вариант тебе подойдет?»

«Я думаю, Annette3».

«Отлично. Тебе рассказать, как его изменить?»

«Нет, я знаю как».

«Хорошо. И последнее, о чем надо поговорить. У тебя на компьютере есть антивирус, который надо регулярно обновлять. Ты не должна отключать автоматическое обновление, даже если твой компьютер временно тормозит. Ладно?»

«Конечно».

«Отлично. У тебя есть наш номер, чтобы ты могла связаться с нами в случае неполадок?»

Номера у нее не было. Он сказал ей номер, и она его аккуратно записала, и вернулась к работе, опять довольная, что о ней заботятся.

Анализ обмана

Эта история затрагивает основную тему, которая

упоминается на протяжении всей книги: чаще всего, информация, которую социальный инженер хочет получить от работника, не знающего о его конечной цели, это аутентификационные данные жертвы. Зная имя пользователя и пароль одного из пользователей, который находится в нужной части компании, атакующий получит то, что ему нужно, чтобы попасть вовнутрь и найти любую нужную ему информацию. Обладать этими данными – то же самое, что найти ключи от города; с ними в руке, он сможет свободно ходить по корпоративному пространству и найдет сокровище, которое он ищет.

Сообщение от Митника

Прежде, чем новым сотрудникам будет разрешено получить доступ к компьютерным системам, они должны быть обучены правилам безопасности, в особенности правилам о нераскрывании паролей.

Не так безопасно, как думаешь

«Компания, которая не прикладывает усилий для защиты важной информации просто поступает небрежно». Многие люди согласятся с этим утверждением. И мир был бы более приятным местом, если бы жизнь была бы более простой и очевидной. Правда в том, что даже те компании, которые прикладывают усилия для защиты конфиденциальной информации, так же могут быть в опасности.

История Стива Крэмера

Эта не была большая лужайка, из тех, с дорогими саженцами. И она явно не была достаточно большой, чтобы дать повод для нанимания косильщика на постоянную работу, что его вполне устраивало, потому что он все равно ой не пользовался. Стив наслаждался подстриганием травы ручной газонокосилкой, и это предоставляло ему убедительное оправдание, чтобы сфокусироваться на его собственных мыслях вместо того, чтобы слушать рассказы Анны о людях в банке, с которыми она работала, или объясняла ему очередные поручения. Он ненавидел записки вроде «Дорогой, сделай…», которые стали неотъемлемой частью его выходных. В его голове вспыхнуло, что его 12-летний сын Пит очень умный и пойдет в команду по пла-

ванью. Но теперь ему придется ходить на тренировки или встречать его каждое воскресенье, так что он не будет настолько застревать с субботней уборкой.

Некоторые люди могут подумать, что работа Стива по созданию новых устройств для GeminiMed Medical Products была скучной; Стив же знал, что он спасает жизни. Стив считал, что он занимается творческой работой. Художник, композитор, инженер – все они, с точки зрения Стива, стояли перед одним и тем же испытанием, что и он: они создавали нечто, что никто до них не делал. В последнее время, он работает над новой моделью искусственного сердца, и это станет его величайшим достижением.

Было почти 11-30 в эту субботу, и Стив был раздражен потому, что он еще не закончил стричь траву, и у него не было новых идей в изобретении метода уменьшения энергозатрат в сердце, последнее оставшееся препятствие. Идеальная проблема, над которой можно подумать во время скоса газона, и он еще не придумал решение.

Анна появилась из-за двери. Ее голова была покрыта красным ковбойским платком, который она надевала, когда убиралась.

«Тебе звонят», – она крикнула ему. «Кто-то с работы».

«Кто?» – Стив крикнул в ответ.

«Ральф какой-то. Мне кажется».

Ральф? Стив не мог вспомнить кого-нибудь из GeminiMed по имени Ральф, который мог бы позвонить ему в выходной. Но, похоже, Анна перепутала имя.

«Стив, это Рэймон Перез из техподдержки». Интересно, как же Анне удалось перепутать испанское имя на «Ральфа», подумал Стив.

«Это просто звонок вежливости», говорил Рэймон. «Трое из серверов не работают, возможно, у нас появился червь, и нам придется переустановить драйвера и восстанавливать все из архивов. Мы полностью восстановим Ваши файлы в среду или четверг. Если повезет».

«Абсолютно недопустимо», – Стив сказал, пытаясь не дать своему гневу завладеть им. Как люди могут быть такими глупыми? Они правда думают, что он сможет обойтись без доступа к своим файлам все выходные и большинство недели? «Ни за что. Я сяду за свой домашний терминал через 2 часа, и должен буду получить доступ к своим файлам. Я ясно выражаюсь?»

«Да, да, и каждый, кому я звонил, хочет поставить себя в верх списка. Я остался без выходных, пришел на работу, и выслушиваю жалобы каждого, с кем я говорю».

«У меня жесткие сроки выполнения работы, компания рассчитывает на это; я должен закончить работу сегодня в полдень».

«Мне еще многим надо позвонить, прежде чем я да-

же смогу начать», – выложил Рэймон. «А что если ты получишь свои файлы во вторник?»

"Не во вторник, не в понедельник, а СЕЙЧАС! "– сказал Стив, интересуясь, кому же он еще позвонит, если пункт еще до него не дошел.

«Ладно, ладно», сказал Рэймон, и Стив услышал в его голосе знаки раздражения. «Дай посмотрю, что я смогу для тебя сделать. Ты используешь RM22, верно?»

«RM22 и GM16. Оба».

«Ясно. Я могу кое-как что-нибудь сделать, не потратив много времени – мне понадобится твое имя пользователя и пароль».

Ой , подумал Стив. *Что здесь происходит? Зачем ему мой пароль? Зачем нужно сотрудникам IT спрашивать об этом?*

«Какая там у вас фамилия? Кто ваш начальник?»

«Рэймон Перез. Смотрите, вот что я вам скажу: когда вас принимали на работу, был листок, которого надо было заполнить для получения учетной записи, и ты записал пароль. Я могу посмотреть, что у тебя записано, идет?»

Стив обдумывал это несколько моментов, а потом согласился. Он ждал с растущим нетерпением, пока Рэймон пошел искать документ из архива. В конце концов, снова у телефона, Стив мог слышать, как он шелестит стопкой бумаги.

«Ах, вот оно», в конце концов, сказал Рэймон. «Вы записали пароль „Janice“.»

Дженис, подумал Стив. Так звали его маму, и он иногда использовал его или в качестве пароля, когда заполнял бумаги при приеме на работу.

«Да, верно», – он признался.

«Окей, мы тратим время зря. Вы знаете, что я серьезно, и если вы хотите, чтобы я воспользовался коротким путем и вернул ваши файлы поскорее, вам придется мне помочь».

"Мой ID – s, d, нижнее подчеркивание, cramer – c-r□a-m□e-r. Пароль – «pelican1».

«Я сейчас этим займусь», сказал Рэймон, наконец-то звуча любезно. «Дай мне пару часов».

Стив закончил с газоном, поел, и когда он добрался до компьютера, он обнаружил, что его файлы были действительно восстановлены. Он был доволен собой, потому что справился с недружелюбным парнем из IT, и надеялся, что Анна слышала, насколько утвердительно он звучал. Было бы неплохо устроить парню или его боссу нагоняй, но он знал, что это – одно из тех вещей, до чего у него никогда не дойдут руки.

История Крэйга Коборна

Крэйг Коборн был продавцом в одной высокотехнологичной компании, и делал свою работу очень хорошо. Через некоторое время он начал осознавать, что у него есть навык ощущения покупателя, понимание, где

человек будет сопротивляться, а где у него слабость или уязвимость, которая сильно увеличивала шансы продать товар. Он начал думать о том, как использовать его талант и этот путь привел его к куда более прибыльной области: промышленному шпионажу.

Это было срочное задание. Мне кажется, оно займет немного времени и прибыли хватит, чтобы поехать на Гавайи. А может быть, Таити.

Парень, который нанял меня, не сказал, конечно, кто клиент, но понятно, что это – некая компания, которая хотела догнать соперников за 1 большой и простой прыжок. Все, что мне надо сделать – получить схемы и спецификации изделия для нового устройства под названием искусственное сердце, что бы это ни значило. Компания называлась GeminiMed. Никогда не слышал о ней, но это – состоятельная компания с офисами в полудюжине разных мест – что делает работу гораздо проще, чем в маленькой компании, где есть серьезный шанс, что парень, с которым ты разговариваешь, знает парня, за которого ты себя выдаешь, и знает, что это не ты. Это, как говорят пилоты о столкновении в воздухе, может испортить весь твой день.

Мой клиент послал мне факс, вырезку из медицинского журнала, в котором говорилось, что GeminiMed работают над сердцем с кардинально новой структурой, и она будет называться STH-100. Громко заявив об этом, какой-то репортер уже сделал большую часть

работы за меня. И у меня уже была важная информация даже раньше, чем я начал – название нового продукта.

Проблема первая: получить имена людей из компании, которые работали над STH-100 или нуждаются в просмотре его схем. Так что я позвонил телефонистке и сказал: "я обещал связаться с одним из людей из группы инженеров, но не помню его фамилии, а его имя начиналось на "С". И она сказала, что «у нас есть Скотт Арчер и Сэм Дэвидсон». Я пошел дальше. «Кто из них работает над STH-100?» Она не знала, так что я решил выбрать Скотта Арчера, и она набрала его номер.

Когда он ответил, я сказал «Здравствуй, это Майк, из почтового отдела. У нас посылка для группы разработчиков Искусственное сердце STH-100. Ты случайно не знаешь, кому это отдать?» И он назвал мне имя руководителя проекта, Джерри Мендела. Я даже смог уговорить его посмотреть его номер для меня.

Я позвонил. Мендела не было на месте, но его автоответчик сказал, что он будет в отпуске до 13-го, что означало, что у него целая неделя для катания на лыжах или чего бы то ни было другого, а в его отсутствие можно звонить Мишель по телефону 9137. Какие любезные люди! Очень любезные!

Я положил трубку и позвонил Мишель, и когда она ответила, я сказал: «Это Бил Томас, Джерри сказал

мне, что я должен буду позвонить тебе, когда будет готовы документы, которые он хотел показать своим ребятам из группы. Вы работаете над искусственным сердцем, верно?» Она сказала, что да.

Теперь переходим к сложной части аферы. Если она стала бы подозревать что-то, я был готов выложить карту, что я просто пытался оказать услугу, о которой попросил Джерри. Я сказал: «какой системой вы пользуетесь»?

«Системой»?

«Какими серверами пользуется ваша группа»?

"А", – она сказала, —"RM22. И некоторые из группы также пользуются GM16". Отлично. Мне это было нужно, и я смог спросить у нее, не вызвав подозрения. И это немного смягчило ее перед следующей частью, которую я пытался сделать как можно более обыденно. «Джерри сказал, что вы можете дать мне список адресов электронной почты людей из команды разработчиков», сказал я и задержал дыхание.

«Конечно. Список слишком длинный, чтобы прочитать, можно я тебе его отправлю по e-mail»?

Ой! Любой адрес, который не заканчивается на geminimed.com, будет как огромный красный флаг. «А что если вы мне его отправите по факсу»?

Она была не против.

«Наш факс не в порядке . Я перезвоню как только получу номер другого», я сказал и положил трубку.

Вы можете подумать, что меня могла обременить эта неприятная проблема, но есть еще один обыденный трюк из торговли. Я подождал некоторое время, чтобы мой голос не показался знакомым секретарше, позвонил ей и сказал: «привет, это Бил Томас, наш факс тут не работает, можно отправить к вам факс»? Она сказала «конечно», и дала мне номер.

А потом я просто вхожу и забираю факс, верно? Конечно нет. Первое правило: никогда не посещайте помещения, если это не обязательно. Они будут долго мучаться, пытаясь опознать тебя, если ты просто голос из телефона. И даже если они тебя опознают, то не смогут арестовать. Сложно надеть наручники на голос. Так что я позвонил секретарше через некоторое время и спросил: пришел ли мой факс? «Да», она сказала.

«Слушай», я сказал ей, «мне надо отправить это нашему консультанту. Ты можешь выслать это за меня»? Она согласилась. А почему бы и нет – как может любой секретарь узнать ценную информацию. Она отправила этот факс «консультанту», и мне пришлось сделать сегодняшнюю пробежку до фирмы неподалеку от меня, со знаком «Прием/Отправка факсов». Мой факс должен был прийти раньше, чем я, и он уже ожидал меня, когда я вошел. Шесть страниц за $1.75. За $10 со сдачей, я получил полный список имен и e-mail'ов.

Проникая вовнутрь

Так, значит мне пришлось поговорить с тремя или

четырьмя разными людьми всего за несколько часов, и уже приблизиться к компьютерам на огромный шаг. Но мне понадобятся еще пару фактов, и все будет сделано.

Во-первых. номер дозвона на инженерный сервер извне. Я позвонил в GeminiMed опять, и попросил соединить с отделом IT, с кем-нибудь, кто помогает с компьютером. Меня соединили, и я начал играть роль смущенного и глупого человека в обращении с техникой. «Я дома, только что купил новый ноутбук, и мне нужно его настроить для доступа извне».

Эта процедура была обычной, но я с нетерпением разрешил ему рассказать все, и вскоре он добрался до номера дозвона. Он назвал мне номер как самую рутинную информацию. И потом, заставил его подождать, пока я пробовал. Идеально.

Так что теперь я преодолел препятствие подключения к сети. Я дозвонился и обнаружил, что они настроили терминальный сервер, который позволяет звонящему подключаться к любому компьютеру в их локальной сети. После кучи попыток, я наткнулся на чей-то компьютер, где был гостевой аккаунт без необходимости ввода пароля. Некоторые ОС, когда они только установлены, заставляют пользователя создать логин и пароль, а также предоставляют гостевой аккаунт. Пользователь должен поставить свой пароль на гостевую учетную запись или отключить ее, но многие даже

не знают об этом или не хотят чего-либо делать. Эта система, скорее всего, была только что установлена, и владелец даже не побеспокоился об отключении гостевого аккаунта.

Благодаря гостевому аккаунту, у меня теперь был доступ к одному компьютеру, на котором оказалась старая версия операционной системы Unix. В Unix'е, операционная система содержит файл, в котором есть зашифрованные пароли каждого, у кого есть доступ к компьютеру. Файл с паролями содержит одностроронний *хэш* (т.е. форма шифрования необратима) пароля каждого пользователя. С хэшем, пароль, к примеру «justdoit» будет представлен в зашифрованном виде; в данном случае, хэш будет конвертирован Юниксом в 13 численно-буквенных символов.

LINGO

хэш – строка беспорядочно записанных символов, которая получается из пароля путем одностороннего шифрования. Процесс теоретически необратим; т.е. считается, что невозможно извлечь пароль из хэша.

Когда Билли Боб из зала захочет перевести какие-либо файлы на другой компьютер, он обязан идентифицировать себя, предоставив логин и пароль. Система, которая проверяет его авторизацию, шифрует его пароль, а потом сравнивает его результат с хэшем, содержащимся в файле с паролем; если они совпадают, ему предоставляют доступ.

Из-за того, что пароли в файле зашифрованы, файл сделан доступным для пользователей, так как, по теории, нет способа расшифровки пароля. И это смешно. Я скачал файл, сделал атаку по словарю(см. главу 12 для более подробного объяснения метода), и выяснил, что один из инженеров, парень по имени Стив Крэмер, в данный момент имел учетную запись на компьютере с паролем «Janice». Я решил попробовать войти с этим паролем на один из серверов разработчиков; он не подошел; если бы все сработало, это бы сэкономило много времени и уменьшило риск. Не помогло.

Это значило, что мне придется обманом заставить парня сказать его имя пользователя и пароль. Для этого мне пришлось дождаться выходных. Вы уже знаете остальное. В субботу я позвонил Крэмеру и рассказал уловку о черве и сервере, которого надо восстановить, чтобы избежать его подозрений.

А что насчет истории, которую я ему рассказал о том, что он заполнял свои бумаги при приеме? Я рассчитывал на то, что он не вспомнит, что этого никогда не было. Новый сотрудник обычно заполняет столько бумаг, что через несколько лет никто не вспомнит. И даже если он меня раскусит, у меня еще был длинный список других имен.

С его именем пользователя и паролем я вошел на сервер, покопался некоторое время, а потом обнаружил файлы со схемами STH-100. Я не был уверен,

какие из них являются ключевыми, так что я перевел файлы на *dead drop* , бесплатный FTP сайт в Китае, где они будут храниться без чьих-либо подозрений. Пусть клиент разбирается в этом мусоре и ищет, что ему нужно.

LINGO

dead drop – место для хранения информации, где вряд ли ее найдут другие. В мире традиционных шпионов, это место могло бы быть за отколотым камнем в стене; в мире компьютерного хакера, это обычно сайт в удаленной стране.

Анализ обмана

Для мужчины, которого мы называем Крэйгом Коборном, или кого-нибудь вроде него, также с опытом в воровском-но-не-всегда-незаконном искусстве социальной инженерии, испытание, представленное здесь, было почти обыденным. Его целью было обнаружить и скачать файлы, находящиеся на безопасном корпоративном сервере, защищенном фаэрволом и всеми обычными техническими средствами.

Большинство его работы было не сложнее, чем поймать дождевые капли в ведро. Он начал с того, что представился кем-то из почтового отдела и добавил ощущение срочности, утверждая, что есть посылка, которую нужно доставить. Этот обман позволил узнать имя руководителя команды инженеров (что полезно для любого социального инженера, который пытает-

ся украсть информацию), создающих искусственное сердце, который был в отпуске – он любезно отставил имя и телефон его ассистента. Позвонив ей, Крэйг рассеял любые подозрения, утверждая, что он выполняет просьбу руководителя проекта. Поскольку руководителя проекта не было в городе, Мишель не могла проверить его утверждения. Она приняла все за правду и без проблем предоставила список людей из группы, что явилось для Крэйга очень важным этапом.

Она даже не заподозрила ничего, когда Крэйг попросил отправить список по факсу вместо электронной почты, обычно более удобной на обеих концах. Почему она была настолько легковерна? Как и многие другие сотрудники, она не хотела, чтобы босс по возвращению узнал, что она отказала звонящему, который просто пытался сделать что-то, о чем попросил ее директор. Кроме того, звонящий сказал, что босс не только разрешил выполнить просьбу, но и попросил помочь. Опять, здесь пример, как кто-то изъявляет сильное желание «играть в команде».

Крэйг избежал риска физического проникновения в здание, просто отправив факс секретарше, зная, что она скорее всего поможет. Секретарей обычно выбираются за очаровательные личные качества и возможность произвести хорошее впечатление. Оказание небольших услуг, отправка и прием факса входит в должность секретарши, и Крэйг хотел извлечь выгоду из это-

го факта. То, с чем она столкнулась – информация, которая могла бы поднять тревогу, если бы кто-нибудь знал ее цену. Но как может она распознать, какая информация безвредна, а какая – конфиденциальна?

Используя другой стиль манипуляции, Крэйг разыгрывал смущение и наивность, чтобы убедить парня в отделе компьютерных операций предоставить dial-up доступ к терминальному серверу компании, используемого в качестве места для подключения к компьютерным системам локальной сети.

Сообщение от Митника

Главная задача каждого сотрудника – сделать свою работу. Под этим давлением, безопасность переходит на второй план и игнорируется. Социальные инженеры рассчитывают на это, когда занимаются своим искусством.

Крэйг смог с легкостью подключиться, используя стандартный пароль, который никогда не менялся, один из бросающихся в глаза, широко-открытых пробелов, которые существуют во многих локальных сетях, которые основываются на фаэрволах. На самом деле, стандартные пароли многих операционных систем, роутеров и других продуктов, включая PBX, доступны в сети. Любой социальный инженер, хакер, промышленный шпион, а также просто любопытствующий может найти список на **http://www.phenoelit.de/dpl/dpl.html** (Просто невероятно, как облегчает Интер-

нет жизнь тех, кто знает где искать, и теперь *вы* знаете).

Коборн смог убедить осторожного, подозрительного мужчину («Какая там у вас фамилия? Кто ваш начальник?») сообщить его имя пользователя и пароль, чтобы он мог мог получить доступ к серверам, используемым командой разработчиков. Это было аналогично оставлению Крэйга с открытой дверью и возможностью работать с самыми охраняемыми секретами компании, качать схемы нового продукта.

А что если Стив Крэмер продолжил чувствовать нечто подозрительное насчет звонка Крэйга? Это маловероятно, что он решит рассказать о своих подозрениях раньше, чем появится на работе утром в понедельник, что было бы поздно для предотвращения атаки.

И еще один ключ к последней уловке: Крэйг сначала относился безответственно и незаинтересованно к требованиям Стива, а потом изменил интонации, будто он пытается помочь Стиву завершить его работу. В большинстве случаев, если жертва верит, что ей пытаются помочь или оказать услугу, то расстанется с конфиденциальной информацией, которую она защищала бы в другом случае.

Предотвращение обмана

Один из наиболее мощных трюков социального инженера включает «перевод стрелок». Это именно то, что вы видели в этой главе. Социальный инженер создает проблему, а потом чудесным образом ее решает, обманом заставляя жертву предоставить доступ к самым охраняемым секретам компании. А ваши сотрудники попадутся на эту уловку? А вы позаботились о создании и применении специальных правил безопасности, которые могли бы предотвратить такое?

Учиться, учиться и еще раз учиться

Есть старая история о туристе в Нью-Йорке, который остановил мужчину на улице и спросил: «Как пройти к Carnegie hall»? Мужчина ответил: «Тренироваться, тренироваться, тренироваться». Все уязвимы к атакам социальных инженеров, и единственная эффективная система защиты компании – обучать и тренировать людей, давая им необходимые навыки для распознавания социального инженера. А потом постоянно напоминать людям о том, что они выучили на тренировке, но способны забыть.

Все в организации должны быть обучены проявлять некоторую долю подозрения при общении с людьми, которых они не знают лично, особенно когда кто-либо

просит любой вид доступа к компьютеру или сети. Это естественно для человека – стремиться доверять другим, но как говорят японцы, бизнес это война. Ваш бизнес не может позволить себе ослабить защиту. Корпоративная техника безопасности должна четко отделять положенное и не положенное поведение.

Безопасность – не «один размер на всех». Персонал в бизнесе обычно разделяет роли и обязанности, и у каждой должности есть свои уязвимости. Должен быть базовый уровень обучения, который надо пройти всем в компании, но кроме того каждый сотрудник должен быть обучен в соответствии со своим профилем работы придерживаться некоторых процедур, которые уменьшают вероятность возникновения упомянутых в этой главе проблем. Люди, которые работают с важной информацией или поставлены на места, требующие доверия, должны получить особое специализированное обучение.

Безопасное хранение важной информации

Когда к людям подходит незнакомец и предлагает свою помощь, как описано в историях в этой главе, работники должны опираться на технику безопасности компании, которая создана в соответствии с нуждами бизнеса, размером и видом вашей компании.

Заметка

Лично я не считаю, что бизнес должен разрешать любой обмен паролями. Гораздо проще выработать

жесткое правило, которое запретит персоналу использовать общий пароль или обмениваться ими. Так безопасней. Но каждый бизнес должен учитывать его специфику и соответствующие меры безопасности.

Никогда не сотрудничайте с незнакомцем, который просит вас посмотреть информацию, набрать незнакомые команды на компьютере, изменить настройки ПО, или, самое разрушительное из всего – открыть приложение к письму или скачать непроверенную программу. Любая программа, даже та, которая, на ваш взгляд, ничего не делает, может не быть настолько невинной, как кажется.

Есть некоторые процедуры, о которых, независимо от качества нашего обучения, мы часто имеем тенденцию забывать через определенное время. Часто мы забываем наше обучение в то время, когда оно нам как раз нужно. Вы можете подумать, что о том, что нельзя выдавать свое имя пользователя и пароль знают все(или должны знать) и практически не надо напоминать об этом: это просто здравый смысл. Но на самом деле, каждому сотруднику надо постоянно напоминать, что сообщение имени пользователя и пароля к офисному или домашнему компьютеру и даже устройству в почтовом отделе эквивалентно сообщению PIN-кода карточки ATM.

Часто возникают достоверные ситуации, когда это необходимо, а возможно даже важно дать кому-ли-

бо конфиденциальную информацию. По этой причине, надо сделать четкое правило о «никогда не…» При этом, в ваших правилах безопасности и процедурах должны быть особенности об условиях, при которых работник может сообщать его или ее пароль и, самое главное – кому разрешено спрашивать эту информацию.

Учитывай источник

Во многих организациях должно существовать правило, что любая информация, которая может причинить вред компании или сотруднику, может быть выдана только тому, с которым сотрудник, владеющий информацией знаком в лицо или чей голос настолько знаком, что вы узнаете его без вопросов.

В высокобезопасных ситуациях, единственные просьбы, которые можно выполнять – это те, которые получены лично или с серьезным подтверждением, к примеру, две отдельных вещи, как общий секрет и временной жетон (time-based token).

Процедуры классификации данных должны предусматривать, что никакая информация не должна быть предоставлена из отдела организации, работающего с секретами, кому-либо, не знакомому лично или подтвержденному каким-либо способом.

Заметка

Удивительно, но даже если проверить имя и телефон звонящего в базе данных о сотрудниках компании

и перезвонить ему, не будет гарантии, что социальный инженер не добавил имя в базу данных компании или не перенаправляет звонки.

Так как же разобраться со звучащей вполне законно просьбой об информации от другого сотрудника компании, вроде списка имен и адресов электронной почты людей из вашей группы? На самом деле, как можно усилить бдительность, когда подобная вещь гораздо менее ценна, чем, скажем, листок о разрабатываемом продукте, и должна применяться только для внутреннего использования? Одна основная часть решения: назначить сотрудников в каждом отделе, которые будут работать со всеми просьбами об отправке информации вне группы. Тогда этим сотрудникам должна быть предоставлена усовершенствованная программа обучения по безопасности, чтобы они знали об особенных процедурах удостоверения личности, которым им надо следовать.

Ни о ком не забывайте

Кто угодно может быстро назвать отделы в своей компании, которые нуждаются в высокой степени защиты от вредоносных атак. Но мы часто не обращаем внимание на другие места, которые менее очевидны, но более уязвимы. В этих рассказах, просьба отправить факс на номер внутри компании казалась невинной и достаточно безопасной, но атакующий извлек выгоду из этой лазейки в безопасности. Здесь урок та-

ков: каждый, от секретаря и административного ассистента до руководителей и менеджеров должны получать специальное обучение, чтобы быть готовым к такому виду трюков. И не забывайте охранять переднюю дверь: секретари часто являются главными мишенями для социальных инженеров и должны быть поставлены в известность об обманных техниках, используемых некоторыми посетителями и звонящими.

Корпоративная безопасность должна четко выработать единый вид контактов, вроде центральной «расчётной палаты» для сотрудников, которым кажется, что они могли стать жертвой уловки социального инженера. Имея единое место для сообщения об инцидентах предоставит эффективную, заранее предупреждающую систему, которая сделает все правильно, когда произойдет скоординированная атака, и можно мгновенно уменьшить возможный ущерб.

Глава 6: «Не могли бы Вы помочь?»

Перевод: Artem (artem sib@inbox.ru)

Вы знаете, как социальные инженеры обманывают людей, предлагая им свою помощь. Другой излюбленный подход основан на обратном: социальный инженер делает вид, что нуждается в помощи другого человека. Мы можем сочувствовать людям в затруднительном положении, и подход оказывается эффективным снова и снова, позволяя социальному инженеру достигнуть своей цели.

Чужак

История в главе 3 показала, как атакующий может служащего сообщить свой (табельный) номер. В этой истории применяется другой подход, чтобы добиться того же результата, и показывает, как атакующий может им воспользоваться.

Наравне с Джонсами

В Силиконовой долине есть некая мировая компания, название которой упоминаться не будет. Отделы сбыта и другие подразделения, расположенные по всему миру, соединены со штаб-квартирой компании посредством глобальной сети (WAN). Взломщик, проворный малый по имени Брайан Аттерби (Brian Atterby), знал, что почти всегда легче проникнуть в сеть в одном из отдаленных мест, где уровень безопасности должен быть ниже, чем в головном офисе.

Взломщик позвонил в офис в Чикаго и попросил соединить с мистером Джонсом. Секретарь в приемной спросила, знает ли он имя мистера Джонса; он ответил: «Оно где-то здесь, я ищу его. Сколько у вас работает Джонсов?». Она сказала: «Три. В каком он подразделении?» Он сказал: «Если вы зачитаете мне имена, может, я вспомню его».

– Барри, Джозеф и Гордон.

– Джо. Я вполне уверен, что это он. И… в каком он подразделении?

– Развития бизнеса

– Отлично. Соедините меня с ним, пожалуйста.

Она соединила его. Когда Джонс взял трубку, атакующий сказал: «Мистер Джонс? Это Тони из отдела (начисления) заработной платы. Мы как раз выполняем ваш запрос о переводе ваших денег на кредитный счет».

– ЧТО?! Вас обманули. Я не делал таких запросов. У меня даже нет счета.

– Проклятие, я уже выполнил запрос.

Джонс был в смятении от мысли, что его деньги могли отправиться на чей-нибудь счет, он начал думать, что парню на том конце провода не следовало торопиться. Прежде чем он успел ответить, атакующий сказал: «Я понимаю, что произошло. Изменения вносятся по номеру служащего. Какой у вас номер?»

Джонс сообщил свой номер. Звонивший сказал: «Действительно, вы не делали запрос».

«Они становятся все более бестолковыми с каждым годом», – подумал Джонс.

«Я внесу исправление прямо сейчас. Не беспокойтесь, вы получите вашу зарплату без проблем», – заверил парень.

Командировка

Почти сразу после этого позвонили системному ад-

министратору в отдел сбыта в Остине, Техас.

«Это Джозеф Джонс, – представился звонивший. – Я из отдела развития бизнеса. Я буду в отеле Дрискил (Driskill Hotel) через неделю. Мне нужна временная учетная запись, чтобы я мог получать электронную почту, не делая междугородных звонков».

«Повторите имя и сообщите мне свой номер», – сказал системный администратор. Лже-Джонс дал ему номер и продолжил: «У вас есть высокоскоростные номера?».

«Подожди, приятель. Я должен проверить тебя по базе данных». Через некоторое время он сказал: «О.К., Джо. Скажи мне номер дома».

Атакующий тщательно подготовился и держал ответ наготове.

Сообщение от Митника

Не надейтесь, что сетевая защита и брандмауэры защитят вашу информацию. Следите за самым уязвимым местом. В большинстве случаев вы обнаружите, что уязвимость заключается в ваших людях.

«О.К., – сказал системный администратор, – ты убедил меня».

Это было просто. Системный администратор проверил имя «Джозеф Джонс», подразделение, номер, и « Джо» сообщил ему правильный ответ на тестовый вопрос. "Имя пользователя будет таким же, как и корпоративное, «jbjones», – сказал системный администра-

тор, – и начальный пароль «changeme» («смени меня»).

Анализ обмана

С помощью пары звонков и 15 минут атакующий получил доступ к глобальной сети компании. В этой компании, как и во многих организациях, было то, что я называю «*слабой безопасностью* » (candy security), термином впервые использованным двумя исследователями из Bell Labs, Стивом Белловином (Steve Bellovin)и Стивеном Чесвиком (Steven Cheswick). Они описывали такую безопасность как «крепкая оболочка со слабым центром», похожую на конфеты M&M. Белловин и Чесвик доказывали, что внешней оболочки, брандмауэра, недостаточно для защиты, потому что взломщик способен обойти ее, а внутренние компьютерные системы защищены слабо. В большинстве случаев они защищаются недостаточно надежно.

Данная история подходит под определение. Имея номер для удаленного доступа и учетную запись, атакующему даже не надо было беспокоиться о проникновении через брандмауэр Интернет, и, будучи внутри, он легко мог скомпрометировать большинство систем во внутренней сети.

По моим данным, эта хитрость сработала с одним из крупнейших производителей компьютерных программ. Вы подумаете, что системных администраторов таких компаний, вероятно, учат обнаруживать уловки такого

типа. Мой опыт подсказывает, что никто полностью не защищен от способного и убедительного социального инженера.

Lingo

«Слабая безопасность» (candy security) – термин, введенный Белловином и Чесвиком из Bell Labs для описания сценария безопасности, где внешняя граница, такая как брандмауэр, прочна, но инфраструктура, расположенная за ним, слаба.

Speakeasy security – «прозрачная» безопасность, которая основана на знании, где находится нужная информация, и использовании слова или имени для доступа к информации или компьютерной системе.

«Прозрачная» безопасность (Speakeasy security)

В дни существования – ночных клубов (speakeasies), где разливался джин – потенциальный клиент получал доступ, найдя дверь и постучав в нее. Через несколько минут , открывалось маленькое окошко и показывалось устрашающее бандитское лицо. Если посетитель был «своим», он называл имя завсегдатая (часто было достаточно сказать: «меня отправил Джо»), после чего вышибала открывал дверь и разрешал войти.

Хитрость была в том, что нужно было знать, где находится заведение, так как дверь ничем не выделялась, и хозяева не размещали вывеску, указывающую на свое присутствие.

Я видел это в фильмах

Вот пример из известного фильма, который многие люди помнят. В "*Трех днях Кондора* " главный герой Тернер (роль играет Роберт Рэдфорд) работает с небольшой исследовательской фирмой по контракту с ЦРУ. Однажды он возвращается с обеда и обнаруживает, что всех его сотрудников застрелили. Ему нужно было выяснить, кто это сделал и почему, зная, что в это время те плохие парни разыскивают его.

Позже он сумел узнать телефонный номер одного из парней. Но кто он такой и как найти его? Ему повезло: сценарист, Дэвид Рэйфил, к счастью, снабдил его опытом, который включает подготовку в войсках связи, дающую ему представление о работе телефонных компаний. Располагая номером парня, Тернер точно знает, что нужно делать дальше. В фильме сцена выглядит таким образом:

Тернер повторно соединяется и набирает другой номер

звонок! звонок! Затем:

Женский голос (фрагмент). Служба имен и адресов (CNA – Customer Name and Address bureau). Миссис Колеман.

Тернер. Миссис Колеман, это Гарольд Томас, абонентская служба. Имя и адрес абонента, пожалуйста, для 202-555-7389.

Женский голос (фрагмент). Одну минуту.

(почти сразу)

Леонард Этвуд, Маккенси Лэйн, 765, Мэриленд. (Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland).

Можете вы осознать случившееся, не обращая внимания на то, что сценарист ошибочно использует междугородный код Вашингтона, округ Колумбия, для адреса в Мэриленде?

Тернер, благодаря опыту линейного монтера, знает, по какому номеру надо звонить в офис компании, которая называется «Служба имен и адресов». Служба имен и адресов абонентов предназначена для удобства монтажников и другого персонала компании. Монтажник может позвонить в службу и назвать номер. Служащий сообщит имя и адрес человека, которому принадлежит телефон.

Обман телефонной компании

В реальной жизни номер службы имен и адресов – тщательно охраняемая тайна. Хотя телефонные компании в наши дни не так легко предоставляют информацию, в то же время они используют разновидность «прозрачной» безопасности, которую специалисты по безопасности называют*«security through obscurity»* (безопасность, основанная на незнании). Предполагается, что любой, кто позвонил в службу имен и адресов и владеет соответствующей терминологией (например, «имя и адрес для 555-1234, пожалуйста»), является человеком, имеющим право на получение ин-

формации.

Lingo

SECURITY THROUGH OBSCURITY – неэффективный метод компьютерной безопасности, основанный на содержании в тайне деталей работы системы (протоколы, алгоритмы, внутренние системы). Такая безопасность основана на обманчивом предположении, согласно которому никто за пределами группы посвященных людей не способен обойти систему.

Сообщение от Митника

Безопасность, основанная на незнании, не приносит никакой пользы при отражении атак социальной инженерии. В каждой компьютерной системе в мире есть как минимум один человек, который ее использует. Таким образом, если социальный инженер способен манипулировать людьми, использующими системы, незаметность системы не подходит.

Не нужно было подтверждать свою личность, сообщать свой номер, ежедневно изменяемый пароль. Если вы знали номер и говорили достоверно, то должны получить право на информацию.

Это было не очень основательным предположением со стороны телефонной компании. Единственная мера безопасности, которую они предприняли, – периодическая смена телефонного номера, по крайней мере, раз в год. Несмотря на это, действующий номер в определенный момент времени был широко известен

среди фрикеров, использующих этот удобный источник информации в своих кругах. Хитрость со службой имен и адресов абонентов была одной из первых вещей, которые я изучил во время увлечения фрикингом в юношеском возрасте.

В мире бизнеса и правительства все еще преобладает «прозрачная» безопасность. Вероятно, здесь необходимо обладать знаниями о подразделениях, людях, и терминологии. компании. Иногда все, что требуется знать, – это внутренний телефон.

Неосторожный руководитель

Хотя многие служащие организаций беззаботны, не интересуются или не подозревают об угрозах безопасности, вы предполагаете, что руководитель компьютерного центра корпорации, входящей в Fortune 500, хорошо знает правила безопасности, верно?

Вероятно, вы не предполагали, что руководитель компьютерного центра – тот, кто является частью отдела информационных технологий компании – окажется жертвой явной игры социальной инженерии. Особенно трудно это предположить, когда социальный инженер не более чем шутник, едва вышедший из подросткового возраста. Но иногда ваши предположения могут быть неверными.

Настройка (на радиоволну)

Очень давно было занятное время для многих людей, которые настраивали радиоприемник на частоты местной полиции или пожарного отделения, слушая разговоры об ограблении банка, пожаре в административном здании или погоне по ходу событий. Сведения о радиочастотах, используемых правоохранительными органами и пожарными отделениями, можно было найти в книжных магазинах; сегодня информация о радиочастотах местных, государственных, и, в некоторых

случаях, даже федеральных органов есть в Интернете, в книге, которую можно купить с помощью Radio Shack.

Конечно, это было не просто любопытство со стороны тех, кто слушал эти частоты. Мошенники, грабящие магазин посреди ночи, могли настроить приемник, чтобы слышать, когда полицейская машина направляется к месту происшествия. Торговцы наркотиками могли контролировать деятельность агентов местных органов. Поджигатель мог усилить свое нездоровое удовольствие, устроив пожар и слушая затем весь поток сообщений по радио, в то время как пожарные боролись с огнем.

За последние годы разработки в компьютерных технологиях позволили шифровать голосовые сообщения. По мере того, как инженеры нашли способы разместить на одном кристалле все больше вычислительных мощностей, они начали создавать зашифрованное радиовещание, лишив плохих парней и любопытных возможности прослушивать его.

Дэнни-перехватчик

Энтузиаст сканирования и искусный хакер, которого мы будем звать Дэнни, решил выяснить, не может ли он получить исходный код сверхсекретной программы-шифратора одного из ведущих производителей защищенных радиосистем. Он надеялся изучить код, который позволил бы ему узнать, как прослушивать разговоры правохранительных органов и, возможно, ис-

пользовать технологию так, чтобы даже самым влиятельным государственным органам было сложно отследить его разговоры с друзьями.

Дэнни из темного мира хакеров принадлежат к особой категории, которая находится где-то между просто любопытными, но безобидными, и опасными. Они обладают знаниями эксперта, сочетающимися с озорным желанием хакера вторгаться в системы и сети ради интеллектуального вызова и удовлетворения от понимания, как работает технология. Их электронные трюки со взломом и проникновением – всего лишь трюки. Эти люди, эти «белые» хакеры незаконно проникают в системы ради забавы и доказательства того, что они могут сделать это. Они ничего не воруют, не зарабатывают деньги на своих деяниях, не уничтожают файлы, не разрушают сети или компьютерные системы. Сам факт их присутствия, получения копий файлов, подбора паролей за спиной сетевых администраторов, утирает носы людей, ответственных за оборону от злоумышленников. Умение превзойти других составляет значительную часть удовлетворения.

Придерживаясь такой направленности, наш Дэнни хотел изучить детали тщательно охраняемого продукта компании только, чтобы удовлетворить жгучее любопытство и удивиться искусным новинкам, которые могли быть внедрены в компании. Излишне говорить о том, что разработка продукта были тщательно охра-

няемой производственной тайной, такой же ценной и защищенной, как и все, чем владела компания. Дэнни знал это. И нисколько не беспокоился. Как-никак, это была всего лишь некая большая безымянная компания.

Но как получить исходный код программы? Как оказалось, похищение «драгоценностей» из группы защищенной связи было слишком легким, несмотря на то что компания была одной из тех организаций, где используется *аутентификация по двум условиям* , при которой требуется не один, а два индентификатора для доказательства своей подлинности.

Вот пример, с которым вы уже, возможно, знакомы. Когда к вам приходит новая кредитная карта, вас просят позвонить в компанию-эмитент, чтобы там знали, что карта находится у ее владельца, а не кого-то, кто украл конверт на почте. В наши дни указания на карте, как правило, предписывают звонить вам*из дома* . Когда вы звоните, программа в компании анализирует номер, автоматически определенный на телефонном коммутаторе, через который проходят бесплатные звонки. Компьютер в компании-эмитенте сравнивает телефонный номер звонившего с номером в базе данных владельцев кредитных карт. К тому времени, как служащий возьмет трубку, на его дисплее будет отображена информация о клиенте из базы данных. служащий уже знает, что звонок сделан из дома клиента, .

Lingo

Аутентификация по двум условиям – использование двух разных типов аутентификации для идентификации. Например, человек может идентифицировать себя звоня из определенного места и зная пароль.

Затем служащий выбирает элемент отображаемых о вас данных – чаще всего номер (социального обеспечения), дату рождения, девичью фамилию матери – и задает вам вопрос. Если вы даете правильный ответ, это вторая форма аутентификации, основанная на сведениях, которые вы должны знать.

В компании, выпускающей защищенные радиосистемы, у каждого служащего, имеющего доступ к компьютеру, имелись имя и пароль, которые дополнялись небольшим электронным устройством – Secure ID (безопасный идентификатор). Это то, что называют синхронизируемым жетоном. Такие устройства делаются двух типов: одно из них размером с половину кредитной карты, но немного толще; другое настолько мало, что люди могут присоединить его к связке ключей.

В этом устройстве из мира криптографии имеется маленький шестиразрядный дисплей. Каждые 60 секунд на дисплее отображается новое шестизначное число. Когда человеку нужен доступ к сети, сначала он должен идентифицировать себя как зарегистрированного пользователя, введя секретный PIN-код и число, отображаемое его устройством. Пройдя проверку вну-

тренней системы, он затем должен ввести имя и пароль.

Для получения исходного кода, которого так жаждал юный Дэнни, нужно было не только скомпрометировать имя пользователя и пароль одного из служащих (что не представляет особой сложности для опытного социального инженера), но и добраться до синхронизируемого жетона.

Прохождение аутентификации по двум условиям с использованием синхронизируемого жетона в сочетании с секретным PIN-кодом кажется невыполнимой миссией. Для социальных инженеров задача подобна той, когда игрок в покер, который обладает не просто умением «читать» своих противников.

Штурм крепости

Дэнни начал с тщательной подготовки. Вскоре он собрал вместе достаточно сведений, чтобы выдать себя за настоящего служащего. У него было имя, подразделение, телефонный номер служащего, а также имя и номер телефона руководителя.

Теперь было затишье перед штурмом. По составленному плану Дэнни нужна была еще одна вещь перед тем, как сделать следующий шаг, и это было то, чем он не управлял: ему нужна была метель. Ему нужна была помощь Матушки– природы в виде непогоды, которая бы не позволила работникам добраться до офиса. Зимой в Южной Дакоте тому, кто надеялся на

плохую погоду, не приходилось ждать очень долго. В пятницу ночью началась метель. снег быстро превратился в град, так что к утру дороги были покрыты слоем льда. Это была отличная возможность для Дэнни.

Он позвонил на завод, попросил соединить с машинным залом и связался с оператором, который представился как Роджер Ковальски.

Назвав имя настоящего служащего, Дэнни сказал: «Это Боб Билингс. Я работаю в группе защищенной связи. Я сейчас дома и не могу приехать из-за метели. Проблема в том, что мне нужен доступ к моему компьютеру и серверу из дома, а я оставил безопасный ID в столе. Не могли бы вы принести его? Или кто-нибудь? А потом прочитать мой код, когда надо будет ввести его? Сроки выполнения у моей группы подходят к концу, и у меня нет другого способа закончить работу. И нет способа попасть в офис – дороги слишком опасны.»

Оператор сказал: «Я не могу оставить вычислительный центр» Дэнни завладел ситуацией: «А у вас есть безопасный ID?»

«В центре есть один, – сказал тот, —Мы храним один для операторов на случай крайней необходимости.»

«Послушайте, – сказал Дэнни, —Вы не могли бы оказать мне большую услугу? Можно позаимствовать ваш безопасный ID, когда мне нужно будет войти в сеть? На время, пока опасно ездить по дорогам?»

–Кто вы? – спросил Ковальски. – Для кого вы делаете работу?

–Для Эда Трентона.

–Ах да, я знаю его.

Когда может возникнуть затруднительное положение, хороший социальный инженер проводит нечто большее, чем простое исследование. «Я работаю на втором этаже, – продолжал Дэнни, – рядом с Роем Такером».

Это имя он тоже знал. Дэнни продолжил обрабатывать его. «Будет проще подойти к моему столу и принести мой безопасный ID.»

Дэнни был уверен, что парень не пойдет на это. Прежде всего, он не оставит свое место посреди рабочей смены ради «прогулки» по коридорам и лестницам в другую часть здания. Он также не захочет шариться в столе на чужом месте. Нет, можно было спорить, что он не сделает этого.

Ковальски не хотел ни отказывать парню, нуждавшемуся в помощи, ни соглашаться и быть втянутым в проблему. Поэтому он отложил решение: «Я должен позвонить моему боссу. Подождите». Он отложил трубку, и Дэнни мог слышать, как тот набирает другой номер, и объясняет просьбу. Затем Ковальски сделал что-то необъяснимое: он по-настоящему ручался за человека, назвавшегося Бобом Билингсом. «Я знаю его, – сказал он своему руководителю, – Он работает для Эда Трен-

тона. Можем мы разрешить ему воспользоваться безопасным ID, который есть в вычислительном центре?» Дэнни, державший трубку, был поражен, услышав о неожиданной поддержке в свою пользу. Он не мог поверить своим ушам.

Через несколько минут Ковальски снова взял трубку, сказал: «Мой руководитель хочет поговорить с вами сам», и дал ему имя и номер сотового телефона.

Дэнни позвонил руководителю и повторил историю снова, подробно рассказав о проекте, над которым он работал, и почему его группа должна закончить работу в срок. «Проще будет кому-нибудь подойти к моему столу и взять мою карту, —сказал он. – Я не думаю, что стол заперт, карта должна быть в левом верхнем ящике».

«Хорошо, – сказал руководитель, – думаю, на выходные мы можем разрешить вам использовать безопасный ID из вычислительного центра. Я скажу дежурным, чтобы они считали случайный код, когда вы позвоните», и дал ему PIN-код для использования.

В выходные, каждый раз, когда Дэнни хотел войти в корпоративную сеть, он должен был только позвонить в вычислительный центр и попросить считать шесть цифр, отображаемых безопасным ID.

Работа изнутри

Он был внутри компьютерной системы компании, что дальше? Как Дэнни найти сервер с нужной ему про-

граммой? Для этого он уже подготовился.

Компьютерные пользователи знакомы с телеконференциями, расширенным набором электронных досок объявлений, где одни люди могут поместить вопросы, на которые отвечают другие люди, или найти виртуальных собеседников с общими интересами в области музыки, компьютеров или любой из сотен других тем.

Сообщения, размещаемые в телеконференциях, остаются доступными годами. Например, Google сейчас содержит архив из семисот миллионов сообщений, некоторые из которых были размещены двадцать лет назад! Дэнни начал с адреса **http://groups.google.com**
.

В качестве ключевых слов Дэнни ввел «шифрованная радиосвязь» и название компании, и нашел сообщение годичной давности от служащего. Оно было помещено, когда компания начала разработку продукта, возможно, задолго до того как полицейские ведомства и федеральные органы взяли под контроль радиосигналы.

Сообщение содержало цифровую подпись, дающую не только имя человека, Скотт Пресс, но и номер его телефона и даже название рабочей группы, Группа защищенной связи.

Денни и набрал номер. Это было похоже на – работает ли он в той же организации годы спустя? На работе он в в такую непогоду? Телефон зазвонил один раз,

другой, третий, тогда раздался голос. «Скотт, – сказал он».

Утверждая, что он из IT-отдела компании, Дэнни заставил Пресса (одним из способов, знакомых вам по предыдущим главам) назвать имена серверов, используемых для разработки. На этих серверах мог располагаться исходный код, содержащий патентованный алгоритм шифрования и микропрограммы, используемые в защищенных изделиях компании.

Дэнни приближался все ближе и ближе, и его волнение усиливалось. Он чувстовал напряжение, высшую точку, которое всегда испытывал, успешно сделав то, чего могли достигнуть немногие.

В остаток выходных он мог войти в сеть компании, когда ему бы захотелось, благодаря сотрудничеству с руководителем вычислительного центра. Он знал, к каким серверам обратиться. Но когда он набрал номер, терминальный сервер, на который он вошел, не разрешил ему соединение с системой разработки Группы защищенной связи. Это был внутренний брандмауэр или маршрутизатор, защищавший компьютерные системы группы. Нужно было найти другой способ войти.

Следующий шаг требовал нахальства – Дэнни позвонил Ковальски и пожаловался: «Мой сервер не разрешает мне соединиться», и сказал: «Мне нужна учетная запись на одном из компьютеров вашего отдела, чтобы я мог использовать Телнет для соединения с мо-

ей системой».

Руководитель уже одобрил раскрытие кода доступа, отображаемого на синхронизируемом жетоне, поэтому новое требование не показалось чрезмерным. Ковальски создал временную учетную запись и пароль на одном из компьютеров вычислительного центра и попросил Дэнни «позвонить, когда учетная запись будет больше не нужна, чтобы я удалил ее».

Зайдя с временной учетной записью, Дэнни мог соединиться по сети с компьютерными системами Группы защищенной связи. После часового поиска уязвимости , которая давала ему доступ к главному серверу, он сорвал куш. Очевидно, системный администратор не следил за последними известиями об ошибках безопасности, которые давали удаленный доступ. Зато Дэнни был хорошо осведомлен об этом.

За короткий срок он нашел файлы с исходными кодами и отправил их на сайт, который предоставлял бесплатное место для хранения. Здесь, даже если файлы были бы обнаружены, на его след никогда не смогли бы выйти.

Перед выходом оставался один заключительный шаг: методичное уничтожение своих следов. Он закончил до того как закончилось шоу Джея Лено. Для Дэнни это была очень хорошая работа на выходных. И он ни разу не подвергнул себя риску. Это было опьяняющее возбуждение, даже лучше чем сноубординг или прыж-

ки с парашютом.

Дэнни был пьян той ночью, не от виски, джина, пива, а от могущества и чувства завершенности, приблизившись к чрезвычайно секретной программе.

Анализ обмана

Как и в предыдущей истории, уловка сработала только потому, что один из работников компании слишком охотно принял, что звонящий был действительно служащим, которым он представился. Стремление помочь сотруднику, с одной стороны, является частью того, что смазывает колеса промышленности, и частью того, что делает приятным работу служащих одних компаний с работниками других организаций. Но с другой стороны, эта полезность может быть главной уязвимостью, которую попытается использовать социальный инженер.

Одна деталь в махинации Дэнни была восхитительной. Когда он просил кого-нибудь принести жетон из своего стола, он настаивал на том, чтобы кто-то «принес» его для него. «Принеси» – это команда, которую вы даете своей собаке. Никто не хочет, чтобы ему велели принести что-нибудь. С помощью одного слова Дэнни сделал так, чтобы просьба была отклонена, было принято другое решение, именно то, которое хотелось ему.

Оператор вычислительного центра, Ковальски, был обманут Дэнни с помощью имен людей, которых он

знал. Но почему *руководитель* Ковальски – IT-руководитель, не меньше, – позволил чужаку проникнуть во внутреннюю сеть компании? Просто потому что звонок о помощи может быть мощным убедительным инструментом в арсенале социального инженера.

Сообщение от Митника

Эта история показывает, что синхронизируемые жетоны и простые формы аутентификации не может быть защитой против коварного социального инженера.

Может что-то подобное случиться в вашей компании? Случилось ли уже?

Предотвращение обмана

Может показаться, что один элемент часто упоминается в этих историях – атакующий приспосабливается звонить в компьютерную сеть компании снаружи, минуя служащего, который помогал бы ему, удостоверившись в том, что звонящий действительно является работником, и у него есть право доступа. Почему я так часто возвращаюсь к этой теме? Потому что это правда один из факторов многих атак социальной инженерии. Для социального инженера это самый легкий путь к достижению цели. Почему атакующий должен тратить часы на вторжение, когда он может сделать это с помощью обычного телефонного звонка?

Один из самых мощных методов провести атаку — это обычная уловка с просьбой о помощи, подход, часто используемый атакующими. Вы не хотите, чтобы

ваши служащие перестали быть полезными для коллег и клиентов, поэтому вам нужно вооружить их особыми процедурами подтверждения для всех, кто запрашивает компьютерный доступ или конфиденциальную информацию. Этот способ , служащие могут быть полезными для тех, кто заслуживает помощи, но в то же время защищают информационное имущество и компьютерные системы организации.

Необходимо детально разобрать, какой механизм подтверждения следует использовать в различных случаях. В главе 17 приведен список процедур, есть руководящие принципы для рассмотрения.

Хороший способ удостоверить личность человека, обратившегося с просьбой, позвонить по телефонному номеру, указанному в справочнике компании. Если человек, обратившийся с просьбой, действительно атакующий, проверочный звонок позволит поговорить с настоящим человеком по телефону, пока самозванец не положил трубку, или выйти на голосовую почту служащего, которая позволит сравнить его голос с голосом атакующего.

Если номера служащих используются в вашей компании для проверки подлинности, то они должны тщательно охраняться и не сообщаться чужим людям. То же самое относится ко всем видам внутренних номеров, как телефонные номера, идентификаторы и даже адреса электронной почты.

Корпоративное обучение должно обратить внимание каждого на распространенные случаи принятия неизвестных людей за настоящих служащих на основании того, что они внушительно говорят или хорошо осведомлены. Нет основания полагать, что подлинность не требуется проверять другими способами, только потому что кто-то знает порядки компании или использует внутреннюю терминологию.

Офицеры безопасности и системные администраторы не должны концентрировать свое внимание только на подготовке кого-либо в вопросах безопасности . Они также должны быть уверены, что сами следуют тем же правилам, процедурам и установленным порядкам.

Пароли и т.п., конечно, никогда не должны использоваться совместно, запрет общего использования даже более важен при использовании синхронизирующих жетонов и другими безопасных форм аутентификации. На уровне здравого смысла должно быть ясно, что совместное использование любого из этих элементов нарушает все дело компании, установившей системы . Разделение означает отсутствие ответственности. Если имеет место инцидент с безопасностью или что-то идет не так, вы не сможете определить. кто несет ответственность.

Служащие должны быть знакомы со стратегиями и методами и социальной инженерии, чтобы внимательно анализировать запросы, которые они получают.

Рассмотрите использование ролевых игр как часть обучения безопасности, так чтобы служащие могли лучше понять, как работает социальный инженер.

Глава 7: Фальшивые сайты и опасные приложения

Перевод: ext3 (**www.hackzona.ru**) cha0s@ua.fm

Говорят, что вы никогда не получите ничего просто так.

По-прежнему, предложение чего-либо бесплатного является хорошей уловкой для получения больших доходов в законном ("Но подождите, это еще не всё! Позвоните прямо сейчас и вы получите дополнительно набор ножей! ") и не совсем законном («Купите один акр заболоченных земель во Флориде и второй вы получите бесплатно!») бизнесе.

И большинство из нас так горит желанием получить это что-то, что многих может сбить с толку, заставить не анализировать это предложение или данное обещание.

Мы знаем привычное предупреждение, «предостережение покупателя», но пришло время обратить внимание на другое предупреждение: Остерегайтесь приложений во входящей почте и свободного программного обеспечения. Сообразительный взломщик использует любое доступное средство, чтобы вломиться в корпоративную сеть, включая обращение к нашему естественному желанию получить бесплатный пода-

рок. Вот вам несколько примеров.

«Не желаете ли вы бесплатно ...?»

Также как и вирусы стали бедствием для человечества и врачей с начала времен, так и подходяще названный компьютерный вирус представляет собой ту же угрозу для пользователей современных технологий.

Компьютерные вирусы, которые привлекают к себе внимание и прекращаются, как только становятся в центре внимания, не случайно наносят большой урон. Они являются продуктом компьютерных вандалов.

Люди, очень интересующиеся компьютерами, становятся злобными компьютерными вандалами, прилагающими все усилия, чтобы показать, насколько они умны. Иногда их действия похожи на обряд инициации, предназначенный для того, чтобы произвести впечатление на старших и более опытных хакеров. Главной мотивацией этих людей в написании червей или вирусов является преднамеренное нанесение ущерба. Если их деятельность уничтожает файлы, разрушает полностью жесткие диски, и самостоятельно рассылается тысячам ничего не подозревающих людей, то вандалы раздуваются от гордости за свое достижение. Если вирус вызывает достаточный хаос, чтобы о нем написали в газетах и предупреждения были даже в се-

ти – это еще лучше.

Много написано о вандалах и их вирусах; книги, программное обеспечение и целые компании были созданы, чтобы обеспечить защиту, но мы не будем пытаться выдвигать аргументы против их атак. В данный момент, разрушительные действия вандалов интересуют нас меньше, чем запланированные действия его дальнего родственника – социального инженера.

Это пришло в письме

Скорей всего, вы каждый день получаете нежданные письма, которые содержат в себе рекламные объявления или предложения чего-либо, в чем вы не только не нуждаетесь, но и не хотите. Думаю, вы знакомы с этим. Они обещают советы по размещению капитала, скидки на компьютеры, телевидение, камеры, витамины или путешествия, предлагают кредитные карты, которые вам не нужны, устройство, которое позволит вам бесплатно смотреть платные каналы, пути улучшения вашего здоровья или сексуальной жизни и так далее, и так далее. Но всегда в вашем электронном ящике найдется сообщение, которое заинтересует вас. Может быть, это бесплатная игра или предложение посмотреть фотографии вашего кумира, бесплатный список программ или недорогая условно-бесплатная программа, которая защитит ваш компьютер от вирусов. Что бы ни предлагалось, вам придется скачать файл с товарами, которые это сообщение убеждает вас по-

пробовать.

Или, может быть, вы получаете сообщение с темой «Дон, я соскучилась» или «Анна, почему ты мне не пишешь» или «Привет Тим, это та сексуальная фотография, которую я обещал». Это не может быть ненужным рекламным письмом, думаете вы, потому что оно содержит ваше имя и кажется таким личным. И вы запускаете приложение, чтобы увидеть фотографию или прочитать сообщение.

Все эти действия – закачка программы, о которой вы узнали в рекламном письме, щелканье по ссылке, которая отправит вас на сайт, о котором вы раньше не слышали, запуск приложения от кого-то, кто вам незнаком – это своеобразное начало проблем. Конечно, чаще всего, то, что вы получаете – это то, что вы ожидали или в худшем случае, что-либо отменяющее или обидное, но безопасное. Но иногда то, что вы получаете – это дело рук вандала.

Умышленная отправка вредоносного кода на ваш компьютер – это всего лишь малая часть атаки. Атакующий должен, прежде всего, убедить вас скачать приложение, чтобы атака удалась.

Заметка

Одним из типов программ, хорошо известных в компьютерном подполье, является утилита удаленного администрирования или троян, который дает взломщику полный контроль над вашим компьютером, как будто

он сам сидит за вашей клавиатурой.

Наиболее опасные формы вредоносного кода-это черви типа LoveLetter,SirCam и Anna Kournikova,все они основаны на технике социального инжиниринга и обмане, нашего желания получить что-то просто так. Червь приходит как приложение к письму, предлагающему что-то соблазнительное, например конфиденциальную информацию, бесплатную порнографию или (очень умная уловка) сообщение, в котором говорится, что файл является распиской за какой-то дорогой товар, который вы, предположительно, заказали. Эта последняя хитрость ведет к тому, что вы открываете файл из страха, что с вашей кредитки может быть снята сумма за товар, который вы не заказывали.

Это поразительно, как много людей попадается на эти уловки, даже будучи предупрежденными об опасности запуска приложений; осведомленность об опасности со временем исчезает, оставляя нас уязвимыми.

Определение вредоносных программ.

Другой вид *malware* – вредоносное программное обеспечение, которое добавляет на ваш компьютер программу, работающую без вашего ведома или согласия, или выполняющую задание без предупреждения. Malware могут выглядеть достаточно безобидно, быть, например, документом Word или PowerPoint презентацией или другим документом, имеющим много функций, но они инсталлируют неразрешенную программу.

Например, malware может быть одной из версий Трояна, о котором мы говорили в Главе 6.Будучи однажды установленной на ваш компьютер, она может отправлять всю набранную вами информацию, включая пароли и номера кредиток, взломщику.

Существует два других типа вредоносных программ, которые могут шокировать вас. Программа первого типа может отправлять взломщику каждое сказанное вами в микрофон слово, *даже если вы думаете, что он выключен.* Хуже, если у вас есть веб-камера, тогда взломщик может захватить все, что попадает в обзор напротив вашего терминала, даже если вы думаете, что камера не работает.

LINGO

Malware – на сленге: вредоносные программы, такие как вирус, червь, троян, которые наносят повреждения

Сообщение от Митника

Бойтесь греков, дары приносящих, иначе вашу компанию может постичь участь города Трои. Если у вас есть сомнения, то лучший способ избежать заражения – использовать защиту.

Хакер со злобным чувством юмора может внедрить вам маленькую программку, которая доставит много хлопот вашему компьютеру. Например, она может заставить открываться ваш CD-rom или свернуть файл, с которым вы только что работали. Также это может

быть аудио запись крика на полной громкости посреди ночи. Ничто из вышеперечисленного не покажется вам смешным, если вы пытаетесь поспать или выполнить свою работу… но, тем не менее, они не причиняют урона.

Сообщение от друга

Сценарий может развиваться еще хуже, несмотря на ваши предосторожности. Представьте себе: Вы решили не давать взломщику больше ни единого шанса. Вы больше не собираетесь скачивать какие-либо файлы, за исключением файлов с безопасных сайтов, которым вы доверяете, таких как SecurityFocus.com или Amazon.com.Вы больше не кликаете по ссылкам в электронных письмах от неизвестных адресатов. Вы больше не запускаете приложений в письмах, которые вы не ждали. И вы проверяете страницу вашего браузера, чтобы убедиться, что сайты, которые вы посещаете с целью коммерческих транзакций или обмена конфиденциальной информацией, обладают должным уровнем защиты.

И однажды вы получаете письмо от друга или делового партнера, которое содержит приложение. Ведь не может что-то опасное прийти от человека, которого вы знаете, правда? Особенно, если вы знаете, кого винить, если информация на вашем компьютере была повреждена.

Вы запускаете файл и… БУМ! Ваш компьютер только что был заражен червем или трояном. Но зачем такой поступок будет совершать человек, которого вы

знаете? Потому что не все в этом мире так, как нам кажется. Вы читали об этом: червь проник в чей-то компьютер и разослался всем, кто был записан в адресной книге. Каждый из тех людей получил письмо от кого-то, кого он знал и кому верил, и каждое из этих писем содержало в себе червя, который самостоятельно распространялся, как рябь по глади озера от брошенного камня.

Причина, почему этот метод является таким эффективным, заключается в том, что он следует теории о попадании в двух птиц одним камнем: умение самостоятельно распространяться и вероятность, что оно приходит от известного вам человека.

Сообщение от Митника

Человечество изобрело много замечательных вещей, которые перевернули мир и нашу жизнь. Но на каждое нормальное пользование технологиями, будь то компьютер, телефон или Интернет, кто-то всегда найдет способ злоупотреблять ими в его или ее интересах.

Печально, что, несмотря на высокий уровень развития современных технологий, вы можете получить письмо от кого-то, близкого вам, и все еще думать, а безопасно ли его открыть.

Вариации по теме

В эту эру Интернета, существует вид мошенничества, который перенаправляет вас совсем не на тот вэб-сайт, который вы ожидали. Это случается регулярно и имеет разнообразные формы проявлений. Этот пример является типичным.

С Новым Годом…

Отставной страховой агент по имени Эдгар получил письмо от PayPal, компании, которая предоставляла быстрый и удобный путь совершения он-лайн покупок. Этот вид сервиса очень удобен, когда человек из одной части страны (или мира) покупает что-либо у человека, с которым он не знаком. PayPal снимает деньги с кредитки покупателя и переводит деньги прямо на счет продавца. Будучи коллекционером антикварных стеклянных кружек, Эдгар совершил множество сделок через он-лайн торги eBay. Он часто пользовался PayPal, иногда несколько раз в неделю. В общем, Эдгар был заинтересован в получении письма на выходных 2001 года, которое, казалось, было отправлено от кого-то PayPal, предлагающего ему награду за обновления своего PayPal счета. В письме было написано:

Сезонные поздравления нашим дорогим клиентам PayPal;

В честь прихода Нового Года PayPal желает добавить 5$ на ваш счет!

Все, что вам требуется, чтобы получить в подарок 5$-обновить вашу информацию на защищенном сайте PayPal к 1Января,2002.Год приносит много изменений и, обновив вашу информацию, вы позволите нам продолжать предоставлять вам и другим дорогим клиентам сервис отличный сервис и, между тем, неуклонно придерживайтесь нашей инструкции!

Чтобы обновить вашу информацию прямо сейчас и получить 5$ на ваш PayPal аккаунт, щелкните по этой ссылке: **http://www.paypal-secure.com/cgi-bin**

Благодарим вас за использование PayPal.com и помощь в дальнейшем развитии нашей компании!

От всего сердца желаем вам счастливого Нового Года!

команда PayPal

Заметка о коммерческих веб сайтах

Возможно, вы знаете людей, вынужденных покупать товары он-лайн, даже у таких брендовых компаний, как Amazon и eBay или веб сайтах Old Navy, Target или Nike. По сути дела, они имеют право быть подозрительными. Если ваш браузер использует сегодняшний стандарт 128 битного шифрования, то информация, которую вы посылаете какому-нибудь защищенному сайту, выходит из вашего компьютера зашифрованной. Эта информация может быть расшифрова-

на с большим трудом, но, в принципе ее невозможно взломать разумные сроки, кроме, разве что привлечения Национального Агентства Безопасности (и оно, насколько нам известно, в 98 году, совсем не показало свой заинтересованности в краже номеров кредиток американцев или попытке выяснить, кто заказывает порно-фильмы или странное нижнее белье).

Эти зашифрованные файлы могут быть вскрыты кем-то лишь при достаточном наличии времени и ресурсов. Но реально, какой дурак пойдет на все это, чтобы украсть один номер кредитки, когда множество онлайн компаний совершают ошибку, храня всю финансовую информацию их клиентов незашифрованной в базах данных? Хуже всего то, что достаточное количество таких компаний, которые используют обычную базу данных SQL, плохо разбираются в проблеме. Они никогда не меняют стоящий по умолчанию пароль системного администратора в программе. Когда они доставали программное обеспечение из коробки, пароль был «null», и он по-прежнему «null» сегодня. Так что содержимое базы данных доступно любому в Интернете, кто решит попробовать подсоединиться к серверу базы данных. Эти сайты все время атакуются, и информация воруется, так как нет никого более опытного.

С другой стороны, те же самые люди, которые не делают покупки через Интернет, потому что боятся кражи информации о своей кредитке, не имеют проблем при

использовании той же кредитки в обыкновенном магазине, уплате за ланч, ужин или выпивку. Чеки о снятии денег с кредитки крадутся из этих мест постоянно или вылавливаются из мусорных корзин на задней аллее. И любой недобросовестный клерк или официант может записать ваше имя и информацию о карте или использовать приспособление, легко доступное в Интернете, или устройство, которое считывает информацию с любой кредитки, как только ей проведут через него, для дальнейшего восстановления.

Существуют несколько опасностей в совершении покупок он-лайн, но, возможно, это так же безопасно, как и в обычных магазинах. И компании, обслуживающие кредитки, предоставляют вам ту же защиту, когда вы пользуетесь своей картой он-лайн, если было совершено незаконное снятие денег с вашего счета, вы несете ответственность только за первые 50$.Так что, по-моему, страх покупок в Интернете – это еще одно необоснованное беспокойство.

Эдгар не заметил некоторых особенных знаков, которые были неправильны в этом письме (например, точка с запятой после поздравительной строки и опечатку « дорогим клиентам сервис отличный сервис»). Он щелкнул по ссылке, заполнил информационный запрос – имя, адрес, номер телефона, информацию о кредитке – и сел ждать, когда же 5$ поступят на его счет. Но вместо того, начал появляться список расхо-

дов на товары, которые он никогда не заказывал.

Анализ обмана

Эдгар попался на довольно банальный в Интернете трюк. Это трюк, который можно использовать довольно разнообразно. Один из видов (описан в Главе 9) включает в себя макет формы авторизации, созданный взломщиком, и идентичный настоящему. Разница заключается в том, что фальшивая форма не дает доступа к системе, до которой пользователь пытается добраться, а кроме этого, отправляет его логин и пароль хакеру.

Эдгар попался на трюк, в котором обманщики зарегистрировали веб сайт с именем «paypal-secure.com»-который звучит так, будто бы это защищенная страница законного PayPal сайта, но это не так. Когда он ввел информацию на том сайте, взломщики получили то, что хотели.

Сообщение от Митника

Пока отсутствует полная защищенность, всякий раз, когда вы посещаете сайт, который требует информацию, которую вы считаете личной, убедитесь, что соединение подлинно и зашифровано. И еще более важно не щелкать автоматически «Да» в любом диалоговом окно, которое может отображать информацию о безопасности, такую как неверный, истекший или аннулированный цифровой сертификат.

Вариации по вариации

Как много других путей существует, чтобы ввести в заблуждение пользователей компьютера и заставить посетить фальшивый веб сайт, где они предоставят свою личную информацию? Я не думаю, что у кого-то есть точный ответ на этот вопрос, но фраза «множество и множество» вполне послужит цели.

Несуществующая ссылка

Один трюк используется регулярно. Отправляется письмо с соблазнительной причиной посетить сайт и предоставляется прямая ссылка на него. Кроме этого, ссылка не доставляет вас на сайт, который вы ожидаете увидеть, потому что ссылка только имеет сходство со ссылкой на тот сайт. Вот вам другой пример, который начал использоваться в Интернете, снова злоупотребляя именем PayPal:

www.PayPai.com

В принципе, это выглядит так, будто речь идет о PayPal. Даже если жертва заметит, то может подумать, что это всего лишь незначительная ошибка в тексте, которая переделала "l" в "i". И кто заметит, что в адресе

www.PayPa1.com

используется цифра 1 вместо прописной "L"? Существует достаточно людей, которые допускают опечат-

ки и другие неправильные указания и тем самым прибавляют популярности этой затее ворующих кредитки. Когда люди идут на фальшивый сайт, он выглядит так же, как и сайт, который они ожидают увидеть, и они жизнерадостно вводят информацию об их кредитке. Чтобы провернуть один из этих ужасов, взломщику всего лишь нужно зарегистрировать фальшивое доменное имя, разослать письма и ждать дураков, чтобы обмануть их.

В середине 2002,я получил письмо, по-видимому, являющееся частью из массовой рассылки, которое было помечено от: **Ebay@ebay.com** . Это сообщение показано ниже.

Дорогой пользователь eBay,

Стало известно, что другая группа испортила ваш eBay аккаунт и нарушила наше Пользовательское Соглашение по безопасности, приведенное ниже:

4. Торги и покупка

Вы обязываетесь завершить транзакцию с продавцом, если вы покупаете товар по одной из указанных нами цен или являетесь лицом, предложившим наибольшую цену на торгах, как упомянуто выше. Если вы предложили наибольшую цен в конце торгов и ваша надбавка к цене одобряется продавцом, вы обязываетесь завершить транзакцию с продавцом или транзакция запрещается законом или этим соглашением.

Вы получили это предупреждение от eBay, потому

что нам стало известно, что ваш текущий аккаунт вызвал неприятности с другими членами eBay и eBay требует немедленно подтвердить ваш аккаунт. Пожалуйста, подтвердите ваш аккаунт, иначе он может быть аннулирован. Щелкните по этой ссылке, чтобы подтвердить ваш аккаунт: **http://errorebay.tripod.com**

Созданные торговые марки и брэнды являются собственностью их соответствующих владельцев, eBay и eBay logo являются торговыми марками eBay Inc.

Жертвы, которые щелкали по ссылке, попадали на веб-страницу, очень похожую на страницу eBay. Фактически, страница была хорошо спроектирована, с достоверным логотипом eBay и ссылками «Посмотреть», «Продать», а также другими навигационными ссылками, которые, если щелкнуть по ним, приводили посетителя на настоящий сайт eBay. В нижнем правом углу был также логотип гарантии. Чтобы удержать догадливую жертву, дизайнер даже использовал даже HTML шифрование, чтобы замаскировать, откуда отправлялась предоставленная пользователем информация.

Это был отличный пример предумышленной атаки с использованием компьютера, на основе социальной инженерии. Но все-таки, в ней были некоторые недоработки.

Письмо не было написано очень хорошо; в частности, параграф, начинающийся словами «Вы получили это предупреждение», слишком бестактный и бессмы-

сленный (люди, ответственные за эти мистификации, никогда не нанимают профессионалов, чтобы отредактировать их образец, и это всегда видно). Также, любой, обративший внимание, пришел бы в подозрение, что eBay интересуется информацией клиента компании PayPal; нет ни одной причины, почему eBay будет спрашивать клиента о его личной информации, использующейся другой компанией.

И кто-нибудь, хорошо осведомленный по теме Интернета, вероятно, поймет, что ссылка соединяет не с доменом eBay, а с tripod.com, который предоставляет бесплатный хостинг. Все это говорит о том, что письмо не было законным. Тем не менее, готов поспорить, что нашлось много людей, напечатавших свою личную информацию, включающую номер кредитки, на ту страницу.

Заметка

Почему людям позволяют регистрировать вводящие в заблуждение и неподходящие домены? Потому что, в соответствии с нынешним законом и он-лайн политикой, любой может зарегистрировать любые имена сайтов, которые еще не используются.

Компании пытаются бороться против такого копирования их адресов, но представьте, с чем они сталкиваются. General Motors подала иск против компании, зарегистрировавшей сайт f**kgeneralmotors.com (только без звездочек) и поместившей ссылку на официальный

сайт General Motors. GM проиграла дело.

Будьте бдительны

Будучи отдельными пользователями Интернета, нам нужно быть бдительными, принимая сознательное решение, когда безопасно вводить персональную информацию, пароли, номера аккаунтов, пины и т.д.

Как много ваших знакомых могут рассказать вам, какой из используемых ими сайтов отвечает всем требованиям безопасности? Как много работников в вашей компании знают, чего ожидать?

Каждый , кто использует Интернет, должен знать о маленьком символе, который обычно появляется на какой-нибудь веб – странице и напоминает нарисованный висячий замок. Им следует знать, что когда засов закрыт, это значит, что защищенность сайта гарантирована. Когда засов открыт или изображение замка отсутствует, веб-сайт не отмечен как подлинный и любая информация, открыто передаваемая, не шифруется.

Тем не менее, атакующий, обладающий администраторскими привилегиями в компьютерной системе компании, может изменить или пропатчить код операционной системы, чтобы исказить понимание пользователем ситуации. Например, перепрограммирование инструкций к софту браузера, который позволяет не отображать нерабочее состояние цифрового сертификата страницы, а просто обходить проверку. Или система может быть изменена с помощью руткита, устано-

вив один или больше *бэкдоров* на уровне операционной системы, где их труднее обнаружить.

Безопасное соединение устанавливает подлинность сайта и шифрует передаваемую информацию, так что атакующий не сможет использовать какие-либо перехваченные данные. Вы можете доверять сайту, даже использующему безопасное соединение? Нет, потому что владелец сайта может не быть бдительным в установке всех необходимых патчей или принуждению пользователей или администраторов к использованию хороших паролей. Так что вы не можете допускать мысль, что тот или иной сайт является неуязвимым к атакам.

LINGO

бэкдор – скрытый вход, который обеспечивает секретный доступ к компьютеру пользователя. Также используется программистами в процессе разработки программы, чтобы иметь возможность «зайти» в программу для исправления ошибок

Надежный HTTP(*гипертекстовый протокол передачи*) или SSL обеспечивает автоматический механизм, который использует цифровые сертификаты не только для зашифровки посланной на удаленный сайт информации, но и для обеспечения идентификации (чтобы убедиться в подлинности удаленного сайта). Тем не менее, этот механизм защиты не приемлем для пользователей, не обращающих внимания на правиль-

ность имени сайта, к которому они пытаются получить доступ.

Другой вопрос безопасности, чаще игнорируемый, появляется в виде предупреждающей таблички, в которой говорится нечто вроде «Этот сайт не является безопасным или срок действия сертификата истек. Вы желаете посетить этот сайт?». Многие пользователи Интернета просто не понимают это сообщение и, когда оно появляется, просто щелкают OK или YES и продолжают свою работу, не подозревая, что они вступили на зыбучие пески. Будьте внимательны: на веб-сайте, не использующем безопасный протокол, никогда не вводите какую-либо конфиденциальную информацию, будь это ваш адрес или номер телефона, номера кредитной карты или банковского счета или что-то еще, что вы желаете сохранить в тайне.

Томас Джефферсон сказал, что поддержание нашей свободы требует постоянной бдительности. Для поддержания безопасности в обществе, где информация играет роль денег, требуется не меньше.

Подобающее понимание вирусов

Особая заметка по поводу вирусов: это необходимо как для корпоративной сети, так и для каждого работника, использующего компьютер. Сверх обычной инсталляции антивирусных программ на компьютеры, пользователям явно нужно подключать программное обеспечение (чего многие люди не очень любят де-

лать, так как это замедляет некоторые функции компьютера).

Будучи владельцем антивирусного программного обеспечения, не стоит забывать о еще одной важной процедуре: своевременном обновлении антивирусных баз. Если ваша компания не собирается рассылать программы или обновления каждому пользователю, каждый из них должен нести ответственность за своевременную установку обновлений. Моя личная рекомендация – настроить свойства антивирусных программ таким образом, чтобы они автоматически обновлялись каждый день.

LINGO

Просто представьте, вы все еще уязвимы, несмотря на регулярное обновление антивирусных баз, и также, вы все еще не защищены полностью от вирусов и червей, которые не распознаются антивирусными программами или файлы об их обнаружении еще не опубликованы.

Все работники с привилегиями удаленного доступа со своих ноутбуков или домашних компьютеров обязаны иметь обновленное антивирусное программное обеспечение и персональный файрвол. Искушенный хакер проанализирует общую ситуацию и найдет самое слабое место, по которому и ударит. Напоминание людям с удаленным доступом о своевременных обновлениях и установке файрволов – обязанность каждой

корпорации, потому что вы не можете ожидать, что рабочие, менеджеры, продавцы и другие, не связанные с IT отделом, будут помнить об опасности незащищенности их компьютеров.

Кроме этих шагов, я рекомендую использовать меньше обычных, но больше важных пакетов, которые защищают от троянских атак. На момент написания книги, лучшими из известных программ являются The Cleaner (**www.microsoft.com**) и trojan defence sweep (**www.diamondcs.com.au**).

В заключение, самое важное сообщение о безопасности для всех компаний, которые не сканируют на наличие опасных писем: Мы все имеем тенденцию быть забывчивыми или беспечными в вопросах, которые кажутся второстепенными в плане выполнения нашей работы, поэтому работникам нужно снова и снова напоминать не запускать приложения в письмах, несмотря на то, что они могут быть отправлены отдельным лицом или организацией, которым можно доверять. И управляющим также нужно напоминать работникам, что они должны использовать работающие антивирусные программы и антитроянское программное обеспечение, которое обеспечивает защиту против писем, которые могут содержать в себе разрушающий груз.

Глава 8: Используя чувство симпатии, вины и запугивание

Перевод: ext3 (**www.hackzona.ru**) cha0s@ua.fm

Как обсуждалось в Главе 15,социальный инженер использует психологию влияния в достижении своей цели и исполнения просьб. Опытные социальные инженеры очень сведущи в развитии уловок, симулирующих эмоции, такие как страх, возбуждение или вина. Они делают это, используя психологические рычаги – автоматические механизмы, которые ведут людей к исполнению требований без всякой доступной им информации.

Мы все хотим избежать трудных ситуаций для нас и окружающих. Базируясь на этом позитивном импульсе, атакующий может сыграть на симпатии человека, заставить жертву чувствовать свою вину или использовать запугивание в роли оружия.

Вот вам несколько прогрессивных уроков в известной тактике игре на эмоциях.

Визит в студию

Вы когда-нибудь замечали, как некоторые люди проходят через охрану на танцевальный вечер в отеле, приватную вечеринку, или презентацию книги без всякого билета или приглашения?

В большинстве случаев, социальный инженер может добиться прохода в такие места, о которых вы и не думали, что это возможно. В этом вы убедитесь на примере следующей истории об индустрии создания фильмов.

Телефонный звонок

"«Офис Рона Хилларда. Это Дороти»

«Привет Дороти. Меня зовут Кайл Беллами. Я только что приступил к работе в отделе Анимации в компании Брайана Глассмана. Вы, ребята, занимаетесь совсем другой деятельностью».

«Я понимаю. Я мало работала над другими фильмами, поэтому не являюсь знатоком. Что я могу для вас сделать?»

«Честно говоря, я чувствую себя довольно тупо. В послеобеденное время ко мне должен прийти писатель, но я даже не знаю, с кем буду говорить и как помочь ему влиться в компанию. Люди из офиса Брайана очень милые, но я не хочу лишний раз надоедать им,

как мне сделать это, как мне сделать то. Это как будто я только перешел в старшие классы и не могу найти дорогу в уборную. Вы понимаете о чем я?»

Дороти засмеялась.

«Вам следует поговорить с отделом безопасности. Наберите 7,а потом 6138.Если попадете на Лорен, то скажите, что Дороти просит помочь вам».

«Спасибо, Дороти. И если я не найду уборную, я позвоню вам!»

Они посмеялись над этой фразой и завершили телефонный разговор.

История Дэвида Гарольда

Я люблю фильмы, и когда я переехал в Лос-Анджелес, думал, что повстречаю много людей, работающих в кино – индустрии и они проведут меня на вечеринки и ланчи в студиях. Я был там где-то год, мне исполнилось 26 лет и самое лучшее, чего я достиг – это тур по студии Юниверсал с другими милыми людьми из Феникса и Кливленда. Все подошло к тому, что если бы они не пригласили меня, то я сам сделал бы это. Собственно говоря, так и получилось.

Я купил экземпляр *Лос-Анджелес Таймс* и читал колонку развлечений на ближайшие пару дней, записывая имена продюсеров различных студий. Я решил попробовать пробиться на одну из больших студий. Так, я позвонил на коммутатор и спросил номер офиса продюсера, о котором я прочитал в газете. Голос секретар-

ши звучал по-матерински, так что мне удавалось добиться удачи. Если бы на ее месте была молоденькая девушка, она бы не стала тратить на меня время.

Но эта Дороти, ее голос напоминал человека, который обязательно подберет заблудившегося на улице котенка и чувствует жалость по отношению к коллеге, подавленному на своей новой работе. И конечно, я нашел к ней верный подход. Не каждый день получается обдурить кого-то так, что он даст вам даже больше, чем вы желали. Она дала мне не только имя одного из людей из отдела Безопасности, но и велела сказать девушке, что Дороти просит ее помочь мне.

Конечно, я в любом случае планировал использовать имя Дороти. И это даже лучше. Ведь Лорен даже не побеспокоится, чтобы проверить, существует ли мое имя в списке служащих.

Когда в тот полдень я подъехал к воротам, у них не только было мое имя в списке посетителей, но и место на стоянке для меня. У меня был небольшой ланч с интендантом и мне бы хотелось большего до конца дня. Я даже пробрался на пару сцен и посмотрел, как снимают фильмы. Я был там до 7 часов. Это был мой самый интересный день.

Анализ обмана

Все когда-то были вновь пришедшими служащими. Все мы помним, что было в первый день, особенно когда мы были молодыми и неопытными. Так что, когда

новичок просит о помощи, он может ожидать, что много людей вспомнят о своих первых шагах на этом поприще и протянут ему руку помощи. Социальный инженер знает это и понимает, что может использовать данное знание, чтобы сыграть на симпатиях своей жертвы.

Мы слишком просто позволяем чужакам пробраться в наши компании и офисы. Даже с охранниками на входе и входными процедурами для не служащих компании, какая-нибудь из разнообразных уловок, использующихся в этой истории позволит злоумышленнику получить бэджик посетителя и пройти вовнутрь. А если ваша компания предоставляет сопровождающих для таких посетителей? Это хорошее правило, но оно эффективно лишь в том случае, если ваши работники добросовестно останавливают всех с или без бэджика посетителя, разгуливающего в одиночку. И если он не скажет ничего вразумительного, его стоит передать службе безопасности.

Позволяя чужакам беспрепятственно разгуливать по вашим сооружениям, вы подвергаете опасности частную информацию вашей компании. В наше время, когда угроза терроризма нависает над обществом, это больше, чем просто информация, которой можно рисковать.

«Сделайте это сейчас»

Не каждый, кто использует тактику социальной инженерии, является идеальным социальным инженером. Любой, кто владеет внутренней информацией компании, может принести опасность. Риск тем больше для тех компаний, которые хранят в своих файлах и базах данных персональную информацию служащих, и конечно, большинство компаний именно так и поступают.

Когда рабочие не достаточно образованы или натренированы для распознавания атаки социального инжиниринга, даже самый твердый человек будет вести себя, как та леди в предыдущей истории.

История Дуга

У нас с Линдой все шло не так уж хорошо, так что, когда я встретил Айрин, я знал, что она предназначена для меня. Линда, как… немного… в общем, относится к типу не особо неуравновешенных людей, но может пойти на любой шаг, когда у нее депрессия.

Будучи джентльменом, я вежливо объяснил, что она должна съехать от меня, и помог упаковать ее вещи, даже разрешил прихватить пару дисков, которые принадлежали мне. Как только она ушла, я поехал в магазин за новым дверным замком и поставил его в ту

же ночь. На следующее утро я позвонил в телефонную компанию и попросил изменить мой номер, а также не опубликовывать его нигде. Это сделало меня свободным и позволило продолжать ухаживать за Айрин.

История Линды

Я была готова уехать, но еще не наметила дату. Но никто не любит чувствовать себя отброшенным. Вопросом было лишь то, как дать ему понять, какое он ничтожество.

Это не заставило долго себя ждать. Там была другая девчонка, иначе он не стал бы с такой скоростью паковать мои вещи. Так что я подождала немного и начала звонить ему каждый день поздно вечером. Знаете, такие действия отбивают у людей желание общаться с кем-либо по телефону.

Я дождалась следующих выходных и позвонила в 11 часов вечера в субботу. Только он сменил номер. И этот номер не был опубликован. Это показывает, каким сукиным сыном он был.

Я стала перебирать бумаги, которые забрала с работы домой, когда ушла из телефонной компании. И там это было – я сохранила ремонтный талон с того раза, когда у Дуга были проблемы с телефонной линией, и на распечатке был указан кабель и пара его телефона. Вы можете поменять номер телефона, но пара медных проводов, идущих от вашего дома до офиса включений телефонной компании (мы называем это

Центральным офисом или просто ЦО) останется той же. Набор медных проводов из каждого дома и квартиры идентифицируется по этим номерам, которые называем кабелем и парой. У меня был список ЦО всего города с их адресами и номерами телефонов. Я нашла номер ЦО по соседству с этим ничтожеством Дугом и позвонила, но, разумеется, там никого не было. Где находится коммутаторщик, когда он вам нужен? Разработка плана заняла у меня 20 секунд. Я начала звонить на остальные ЦО и, наконец, застала на одной из них парня. Но я знала, что он находится очень далеко и скорей всего, сидит с задранными на стол ногами. И, конечно же, не захочет выполнить мою просьбу. Но у меня был план.

«Это Линда, Ремонтный Центр» – сказала я. «У нас чрезвычайная ситуация. Вышел из строя сервис для медицинского блока. Мы пытаемся поднять сервис, но не можем найти проблему. Нам нужно, чтобы вы приехали на Вебстер ЦО сейчас же и посмотрели, может ли тоновый набор выйти из ЦО»

И затем я сказала, «Я перезвоню вам, когда вы доберетесь до места», потому что, разумеется, я не могла позволить ему звонить в Ремонтный Центр и спрашивать меня. Я знала, что ему не захочется покидать комфортный ЦО и исполнять мою просьбу, но это была чрезвычайная ситуация, так что он не мог мне отказать.

Когда я обнаружила его на Вебстер ЦО через 45 минут, я сказала ему проверить кабель 29 пару 2481,он ответил, что тоновый набор есть. Это я, конечно же, знала. Затем я говорю: «Отлично, мне нужно, чтобы вы сделали LV»,что значит подтверждение линии, которое запрашивает телефонный номер. Он выполнил это путем дозвона на специальный номер, который считывает и посылает обратно необходимый номер. Он не знал, что это неопубликованный и недавно измененный номер, так что он выполнил мою просьбу, и я услышала номер. Превосходно. Пустышка сработала великолепно. Я поблагодарила его и пожелала спокойной ночи.

Сообщение от Митника

Если однажды социальный инженер узнает, как вещи работают внутри целевой компании, становится очень просто использовать это знание, чтобы наладить связь с законными служащими. Компаниям необходимо готовить к такого рода атакам всех рабочих. Теневые проверки могут помочь определить людей, склонных к данному типу поведения. Но в большинстве случаев, таких людей слишком трудно обнаружить. Единственный выход-это усилить и проверять процедуры идентификации, включая статус рабочего.

Дуг так много сделал, чтобы спрятаться от меня за неопубликованным номером. Веселье только начиналось.

Анализ обмана

Молодая леди в этой истории смогла достать информацию, которая была необходима для осуществления мщения, потому что она владела знанием внутренней работы: телефонные номера, процедуры и жаргон телефонной компании. Обладая этим, она не только смогла найти новый, неопубликованный номер, но и смогла заставить коммутаторщика проехать снежной ночью через весь город ради ее просьбы.

«Мистер Бигг хочет это»

Популярная и высоко эффективная форма запугивания – популярна в больших масштабах, в силу простоты – основывается на влиянии на человеческое поведение, используя авторитет.

Даже просто имя помощника в офисе CEO может быть ценным. Частные сыщики делают это все время. Они позвонят оператору коммутатора и скажут, что хотят подсоединиться к офису CEO.Когда секретарь или главный помощник ответит, они скажут, что у них в наличии имеется документ или пакет для CEO,или если они отправят е-мэйл приложение, распечатает ли она его?

Или иначе, они спросят, какой номер факса? И, кстати, как вас зовут?

Затем они звонят следующему человеку и говорят, «Дженни из офиса мистера Бигса сказала, что вы мне можете помочь кое с чем».

Эту технику можно назвать «бросанием имени», и обычно она используется как метод быстрой установки связи путем влияния на человека, которое заключается в том, что цель начинает верить в связь атакующего с кем-то из крупных специалистов. Лучше всего, если цель оказывает услугу кому-либо, кто знаком с тем, ко-

го знает используемый человек.

Если атакующий нацелился на довольно важную информацию, он может использовать такой вариант, как пробуждение нужных эмоций в жертве, таких как страх доставить неприятности кому-либо из вышестоящих. Рассмотрим следующий пример.

История Скотта

«Скотт Абрамс.»

«Скотт, это Кристофер Далбридж. Я только что разговаривал по телефону с мистером Бигли, и надо сказать, что он больше, чем невесел. Он говорит, что десять дней назад передал вашим людям записку об исследовании степени интеграции рынка, которую они должны были откопировать и отправить нам для анализа. И мы ее не получали».

«Исследование степени интеграции рынка? Никто не говорил мне об этом. В каком вы ведомстве?»

«Он нанял нашу консультационную фирму, и мы уже перед сдачей работы».

«Послушайте, я сейчас направляюсь на встречу. Скажите мне свой номер телефона и»…

Фразы атакующего звучат поистине победно: "Это то, что вы хотите, чтобы я сказал мистеру Бигли? Послушайте, завтра утром он ожидает итога работы наших аналитиков и нам придется работать над этим всю ночь. А теперь, вы хотите, чтобы *я* сказал ему, что мы не смогли выполнить работу из-за того, что не полу-

чили заметку от вас, или, быть может, вы сами хотите сказать ему об этом?"

Анализ обмана

Уловка с использованием запугивания со ссылкой на авторитет работает особенно хорошо в том случае, если другой человек имеет достаточно низкий статус в компании. Использование важного человеческого имени помогает не только побороть нормальное чувство подозрения, но и делает человека более внимательным; врожденный инстинкт желания быть полезным увеличивается, когда вы думаете, что персона, которой вы помогаете, важна и влиятельна.

Социальный инженер также знает, что лучший путь использования данного трюка – использовать имя кого-то более вышестоящего, чем босс жертвы. И данный трюк довольно ненадежен, если использовать его внутри малой организации: атакующий не хочет, чтобы его жертва могла отпустить комментарий кому-нибудь из отдела маркетинга. «Я отправил тот план, о котором говорил мне один из ваших парней», – это может легко вызвать встречный вопрос вроде: "Какой план? Какой парень? " И это может привести к открытию, что компания стала жертвой.

Сообщение от Митника

Запугивание может вызвать страх перед наказанием, который заставит людей сотрудничать. Также запугивание может пробудить страх запутаться в делах

или быть вычеркнутым из плана по повышению.

Люди должны знать, что неприемлемо зависеть от чьего-либо авторитета, когда на кону безопасность. Тренировка сотрудников должна включать в себя обучение персонала избегать влияния авторитета в дружеских или деловых отношениях, но без нанесения вреда общению. Более того, такие действия должны приветствоваться высшим руководством.

Что знает о вас администрация общественной безопасности

Нам нравится думать, что правительственные организации хранят данные о нас надежно охраняемые от посторонних. Реальность заключается в том, что федеральные управления не так устойчивы к проникновениям, как нам хочется думать.

Звонок от Мэй Линн

Место: региональный офис администрации общественной безопасности

Время: 10.18 утра, четверг

«Это Мэй Линн Ванг»

Голос на другом конце провода звучал примирительно, почти робко.

«Мисс Ванг, это Артур Арондэйл, офис главного инспектора. Могу я звать вас Мэй?»

«Это – Мэй Линн» – отвечает она.

«Хорошо, это так, Мэй Линн. У нас тут новый парень, у которого нет компьютера и прямо сейчас у него приоритетный проект, поэтому он использует мой. Мы работаем в правительстве Америки, и они нам говорят, что у них нет достаточно денег в бюджете, чтобы купить этому парню компьютер. А сейчас мой босс думает, что я опаздываю с выполнением своей работы, и не

хочет слышать никакие извинения, вы знаете?»

«Я знаю, о чем вы, хорошо»

«Не могли бы вы мне помочь с быстрым запросом на MCS?»-он использует имя системы, где записаны все налогоплательщики.

«Конечно, что вам нужно?»

«Первое, поиск счета на Джозефа Джонсона, дата рождения 07.04.69»

После небольшой паузы она спрашивает:

«Что именно вы хотите знать?»

«Какой номер его счета?»

Она прочитывает его.

«Отлично, теперь мне нужен идентификационный номер на этот счет», говорит звонящий.

Это был запрос на базовую информацию о налогоплательщике, и Мэй Линн говорит место жительства, девичью фамилию матери и имя отца. Звонящий внимательно слушает, пока она говорит ему месяц и год заведения карточки и офис, где она была заведена.

Затем он спрашивает о подробном заработке человека.

Данный запрос вызывает ответ, «За какой год?»

Он отвечает, «за 2001»

Мэй Линн говорит, «он равен $190,286,плательщик Джонсон МикроТек»

«Какие-нибудь другие зарплаты?»

«Нет»

«Спасибо», – говорит он, « вы были очень добры».

Теперь он всегда звонит ей, когда ему нужна какая-либо информация, а у него нет доступа к компьютеру. Он снова использует любимый трюк социальных инженеров, установив связь с человеком однажды – всегда возвращаться к нему, чтобы избежать ненужных поисков.

«Не на следующей неделе», говорит она ему, потому что собирается поехать в Кентукки на свадьбу своей сестры. В любое другое время, когда она будет свободна.

Когда она кладет трубку, Мэй Линн чувствует радость, что хоть немного помогла недооцененному государственному работнику.

История Кейт Картер

Если судить по фильмам и хорошо продающимся криминальным новеллам, частные сыщики отлично разбираются в том, как выудить факты у людей. Они делают это, используя совершенно нелегальные методы. Но, по правде говоря, большинство ЧС ведут законный бизнес. С тех пор, как большинство из них начинали свою работу в роли полицейских, они отлично знают, что легально, а что нет, и большинство из них не желают переступать эту линию.

Но есть, разумеется, и исключения. Некоторые ЧС создают алиби для парней, замешанных в криминальных историях. Эти парни известны на рынке как инфор-

мационные брокеры, утонченное оружие для людей, готовых нарушить законы. Они знают, что могут выполнить любое задание быстрее, если используют некоторые ускоренные методы. Эти ускоренные методы могут являться преступными и отправить этих людей за решетку на несколько лет, но это не пугает некоторых, особенно беспринципных личностей.

Между тем, ЧС уровнем выше среднего – те, кто работают не в шикарных костюмах в офисах, расположенных в самой высокооплачиваемой части города, – не делают такие типы работ самостоятельно. Намного проще нанять информационного брокера, чтобы он сделал все за него.

Парень, которого мы назовем Кейт Картер, был не обременен нормами этики.

Это было типичное дело «Где он прячет деньги?» или иногда «Где она прячет деньги?» Иногда это была богатая женщина, желающая знать, куда муж спрятал ее деньги (вопрос, почему женщина с деньгами выходила замуж за мужчину без них, всегда оставался для Кейта Картера неразрешимой загадкой).

В этом деле муж, которого звали Джо Джонсон, был «очень умным парнем, который открыл компанию, занимающуюся высокими технологиями, стартовав с 10 тысяч долларов, которые одолжил у семьи жены, и в итоге фирма превратилась в много – миллионную компанию». Согласно адвокату, занимающемуся раз-

водом, он произвел изумительную работу по сокрытию своих активов, и все уже сбились с ног, разыскивая их.

Кейт наметил отправной точкой Администрацию общественной безопасности, концентрируя их файлы на Джонсона, которые содержали весьма полезную информацию для ситуации, подобной данной. Вооруженный их информацией, Кейт мог притвориться мишенью и заставить банки, брокерские конторы и оффшорные организации рассказать ему все.

Его первый звонок был в офис местной администрации, номер которой был размещен в телефонной книге. Когда служащий взял трубку, Кейт попросил соединить его с кем-нибудь из отдела подачи исков заказчикам. Еще одна пауза – и, наконец, голос. Кейт изменил схему действия и начал: «Привет. Это Грегори Адамс, местный офис 329.Слушай, я пытаюсь добраться до хранилища, которое содержит номер счета, оканчивающегося на 6363.»

«Это Мод2»,ответил мужчина. Он проверил номер и дал его Кейту.

Затем он позвонил на Мод2.Когда Мэй Линн ответила, он придумал, что звонит из офиса главного инспектора и о проблеме, что кому-то другому приходится сидеть за его компьютером. Она дала ему всю информацию, в которой он нуждался, и пообещала сделать все возможное, если ему понадобится помощь в будущем.

Анализ обмана

Что сделало его попытку эффективной, так это умелая игра на симпатии работника к нему после рассказа истории о занятом компьютере и о том, что «мой босс недоволен мной». Люди не проявляют на работе свои эмоции очень часто, но если они это делают, то успех атакующему обеспечен. И эмоциональная уловка «Я в беде, не могли бы вы помочь мне?» – это все, что нужно, чтобы выиграть.

Общественная незащищенность

Администрация общественной безопасности разместила копию их полного справочника действий в сети, в котором много информации, полезной для их работников, но еще более важной для социальных инженеров. Он содержит аббревиатуры, жаргонизмы и инструкции, как делать запрос относительно интересующей вас информации, как описано в предыдущей истории.

Вы хотите знать больше об Администрации общественной безопасности? Просто поищите в Google или введите следующий адрес в вашем браузере:

http://policy.ssa.gov/poms.nsf/

Несмотря на то, что в агенстве уже прочитали эту историю и удалили руководство к тому времени, как вы читаете эти строки, вы найдете он-лайн инструкции, которые даже дают детальную информацию о том, какие данные служащий АОБ вправе давать определенному кругу людей. Практически же, этот круг включает в себя любого социального инженера, который может убе-

дить служащего, что он из законной организации.

Атакующий не сможет добиться успеха в добыче информации у служащего, который отвечает на звонки всех людей. Тип атаки, использованной Кейтом, работает лишь тогда, когда человек получает конец разговора с кем-то, чей номер телефона не доступен широкой публике и к тому же создается впечатление, что тот, кто звонит, работает в компании. Элементы, которые сделали эту атаку возможной:

знание номера телефона Мод

владение необходимой терминологией

выдумка, что он из офиса главного инспектора, о котором каждый государственный служащий знал как об агентстве, обладающем властью. Это дает атакующему некую ауру авторитета.

Одна интересная деталь: кажется, что социальные инженеры знают, как правильно делать запросы, так что никому и в голову не придет подумать, "Почему вы звоните *мне?* " – даже тогда, когда с точки зрения здравого смысла будет логичней обратиться к другому человеку из другого департамента. Возможно, это работает потому, что разрушает чрезмерную обыденность рабочего дня, и звонок кажется чем-то необычным.

И в завершение, атакующий не удовлетворяется разовым получением информации, но и желает установить более прочный контакт, которым можно будет воспользоваться в будущем. Он мог использовать другие

уловки, вроде «Я пролил кофе на клавиатуру». Но в данной ситуации это было бы плохой идеей, так как клавиатуру можно поменять очень быстро.

Итак, он использовал историю о ком-то другом, использующим его компьютер, которая могла растянуться на недели: «Да, я думал, что вчера ему дадут компьютер, но кто-то более ловкий договорился и забрал компьютер себе. Так что этот шутник все еще находится на моем месте»… И так далее.

Какой же я несчастный, мне нужна помощь. Эти фразы заколдовывают.

Один простой звонок

Один из главных барьеров для атакующего – заставить звучать свой запрос обоснованно и типично, чтобы сильно не выделяться в течение рабочего дня жертвы. Как и с другими вещами в нашей жизни, составление правильного запроса может быть соревнованием сегодня, а завтра куском торта.

Телефонный звонок Мэри Х'з

Дата / Время: понедельник, 23 ноября,7.49 утра

Место: Мауэрсбай и Сторч бухгалтерия, Нью-Йорк

Для большинства людей бухгалтерия-это процесс подсчета денег, который так же приятен, как и root аккаунт. К счастью, не все рассматривают работу с этих позиций. Мэри Харрис, например, находит свою работу захватывающей, и это-часть причины, почему она считается одной из лучших служащих в своей фирме.

В этот обычный понедельник, Мэри приехала на работу в ожидании длинного рабочего дня и была очень удивлена телефонным звонком. Она подняла трубку и представилась.

«Привет, это Питер Шеппард. Я из Arbuclde Support,компании, которая занимается технической поддержкой вашей фирмы. Мы получили несколько жалоб за выходные от людей, у которых были про-

блемы с компьютерами. Я подумал, что мне следует узнать все ли в порядке, перед тем, как все выйдут на работу. У вас не было проблем с компьютером или с подключением к сети?»

Она ответила, что еще не знает. Она включила компьютер, и пока он загружался, он объяснил, что от нее требуется.

«Нужно, чтобы мы сделали парочку тестов. Я могу видеть на своем мониторе то, что вы печатаете, и мне нужно проверить, не нарушается ли это во время работы сети. Так что каждый раз, когда вы печатаете строку, говорите мне, что это, чтобы я мог сравнить. Хорошо?»

С ночными кошмарами о сломанном компьютере и потерянном впустую дне, она была более чем счастлива от предложения помощи. После нескольких моментов она сказала ему: «Передо мной экран идентификации, и я собираюсь ввести свой логин. Я печатаю его сейчас М Э Р И Д»

"Отлично, "ответил он. "Я все вижу. Далее, напечатайте свой пароль, но не говорите мне его. Вы никогда не должны говорить кому-либо свой пароль, даже тех. службе. Я лишь увижу звездочки у себя – ваш пароль защищен, так что я не могу увидеть его. "Ничего из вышесказанного не было правдой, но это повлияло на Мэри. И затем он сказал: «Скажите мне, когда ваш компьютер включится».

Когда она сказала об этом, он попросил ее запустить

два приложения, и она ответила, что они работают нормально.

Для Мэри было большим облегчением, что компьютер работает нормально. Питер сказал: «Я рад, что смог убедиться в работоспособности вашего компьютера. Послушайте», – он продолжил", мы только что установили обновление, которое позволит людям менять их пароли. Не могли бы вы потратить еще парочку минут и проверить, правильно ли оно работает?"

Она была благодарна за помощь и потому с радостью согласилась. Питер помог ей запустить приложения, позволяющие поменять пароль, стандартные элементы ОС Windows 2000."Давайте дальше и введите свой пароль" – сказал он ей. «Но не произносите его вслух».

Когда она сказала, что выполнила задачу, Питер ответил, "Для быстрой проверки, когда у вас запросят пароль, напишите «test123».Затем подтвердите его и нажмите enter "

Он провел ее через процесс отсоединения от сервера. Он попросил ее подождать пару минут, затем присоединиться вновь, пытаясь в это время использовать ее новый пароль. Это работало, как по мановению волшебной палочки, Питер казался очень услужливым, и посоветовал ей сменить пароль на свой прежний или выбрать более безопасный пароль и так же не произносить его вслух.

«Отлично Мэри», – сказал Питер. "Мы не обнаружили никаких сбоев, и это здорово. Послушайте, если какие-то проблемы все же возникнут, просто позвоните на Arbucle. Обычно я принимаю участие в особых проектах, но кто-нибудь обязательно поможет вам. " Она поблагодарила его и они попрощались.

История Питера

Вокруг Питера ходили определенные слухи – когда он еще учился в школе, его товарищи знали, что он был кем-то вроде компьютерного мага, который мог достать любую информацию. Когда Элис Конрад обратилась к нему за помощью, сначала он отказался. С какой это стати он должен ей помогать? Когда он ухаживал за ней и пригласил на свидание, она ответила ему довольно прохладно.

Но его отказ помочь не удивил ее очень сильно. Она говорила, что отсутствует гарантия, что он выполнит ее просьбу, но это было как приключение. И вот как он все-таки согласился.

Элис заключила контакт с маркетинговой фирмой на должность консультанта, но положения контракта ее не устраивали. Перед тем, как изменить свой договор, ей хотелось узнать, на каких условиях работают другие консультанты.

Вот то, как Питер рассказывает эту историю.

Я не сказал Элис, что был знаком с людьми, которые не ожидали, что я могу провернуть некоторые делиш-

ки, а для меня это было сущим пустяком. Конечно, не совсем пустяком, но достаточно просто. Ее дело тоже было не слишком трудным.

Где-то после 7. 30 утра в понедельник, я позвонил в маркетинговую компанию и разговаривал с регистратором, сказав, что я работаю в компании, занимающейся планированием их пособий и мне нужно связаться с кем-нибудь из бухгалтерии. Не знает ли она, кто-нибудь уже пришел? Она ответила, «Мне кажется, я видела Мэри. Я отправлю вас к ней».

Когда Мэри подняла трубку, я рассказал ей мою маленькую историю про компьютер, которая позволила расположить ее ко мне. Пока я объяснял, как сменить пароль, я быстро залогинился под этим временным паролем в системе.

Затем, я установил небольшую программу, дающую доступ к их компьютерной системе в любое время. После того, как я попрощался с Мэри, моим первым действием было замести следы, так что никто не мог узнать о моем пребывании в системе. Это было просто. После повышения моих привилегий, я мог скачать простую программку для очистки логов с сайта **www.ntsecurity.nu**

Затем пришло время для настоящей работы. Я запустил поиск любых документов по ключевому слову «контракт» и скачал эти файлы. Затем я поискал еще немного и зашел в основную директорию, где храни-

лись все финансовые отчеты. Так что я сложил вместе файлы контактов и списки платежей.

Элис могла изучить контакты и увидеть, сколько они платят другим консультантам. Разбирать все эти файлы – это ее работа. Свою задачу я выполнил.

Я распечатал некоторые файлы, которые скопировал себе на диск, чтобы она поверила. Я попросил ее встретить меня и купить обед. Вы бы видели ее лицо, когда она увидела кипу бумаг. «Не может быть,» – сказала она, «не может быть».

Я не принес диски с собой. Они были для нее приманкой. Я сказал, что ей придется зайти ко мне, чтобы забрать их. Разумеется, я надеялся, что она выскажет свою признательность за оказанную мной услугу.

Сообщение от Митника

Это удивительно, как многого может добиться социальный инженер, правильно составляя свой запрос. Основная предпосылка-привлечение человека автоматически к ответу, базируясь на психологических принципах, и способность положиться на ментальные особенности человека, принимающего звонящего за своего союзника.

Анализ обмана

Звонок Питера в маркетинговую компанию представляет собой наиболее основную форму социальной инженерии – простой запрос, который требует небольшой подготовки, базирующийся на первом подходе и

занимающий пару минут.

Так что у Мэри не было основания предполагать, что ее обманули.

Это дело прошло успешно благодаря трем тактикам. Первое, он сыграл на чувству страха Мэри – заставил ее подумать, что компьютер может сломаться. Затем он дал ей время запустить пару приложений, так что она могла убедиться, что все работает нормально. Затем, он сыграл на ее чувстве благодарности за помощь в проверке компьютера.

Не позволяя ей произнести новый пароль вслух, даже ему, Питер укрепил ее во мнении, что безопасность компьютерной системы фирмы играет для него большую роль. Это укрепило ее уверенность, что он – законный работник, так как защищает ее и компанию.

Полицейский набег

Представьте себе такую картину: Правительство пытается поймать человека по имени Артуро Санчез, который распространяет бесплатно фильмы через интернет. Голливудские компании утверждают, что он нарушает их права, а он считает, что лишь пытается подтолкнуть их к решению о размещении фильмов в сети для скачки. Он делает вывод, что такое действо может стать хорошим источником доходов для студий, которые обычно игнорируются всеми.

Ордер на обыск, пожалуйста

Придя поздно ночью домой, он еще издалека заметил, что окна в его квартире не горят, хотя в одном из них он оставлял свет.

Он разбудил соседей и выяснил, что в здании был совершен полицейский рейд. Но они заставили всех жильцов выйти на улицу, и никто не знал, в чьей квартире они устроили засаду. Он только мог добавить, что они выносили какие-то тяжелые предметы. И они не выводили никого в наручниках.

Артуро проверил свою квартиру. Плохой новостью было уведомление из полиции, чтобы он связался с ними через три дня. А еще худшей новостью было то, что они забрали все его компьютеры.

Артуро растворился в ночи, оставшись ночевать у своего друга. Но неизвестность мучила его. Как полиция все узнала? Неужели они следили за ним, но дали ему шанс уйти? Или случилось что-то другое? А может ли он предпринять что-то, чтобы не уезжать из города?

Прежде чем читать дальше, остановитесь и задумайтесь: Вы можете представить, каким образом полиция может пронюхать про вас все? Учитывая, что вы не засветились в политической деятельности, у вас нет друзей в полиции, каким образом они могут знать о вас, простом горожанине, всю информацию? Или это постарался социальный инженер?

Обдуривая полицию

Артуро удовлетворил свою потребность в информации следующим способом: для начала, он нашел номер ближайшего магазина видео-проката, позвонил им и узнал номер их факса.

Затем он позвонил в адвокатскую контору и запросил отдел по записям. Когда его соединили, он представился следователем округа Lake и заявил, что ему необходимо переговорить с клерком, хранящим информацию о доказательствах.

«Это я», – ответила женщина. «О, отлично», – сказал он. «Дело в том, что прошлой ночью был рейд в квартире подозреваемого и сейчас я пытаюсь найти показание присяжного».

«Мы располагаем информацию по адресу», – отве-

тила она ему.

Он дал ей свой адрес, и ее голос зазвучал взволнованно. «О, да», – выдохнула она, «Я знаю о чем речь. Дело о нарушении авторских прав».

"Да, то самое. Я ищу показание присяжного и копию уведомления. "

"Отлично, они совсем недалеко. "

«Великолепно. Послушайте, я сейчас не на рабочем месте и через 15 минут у меня встреча по этому делу. И я был настолько рассеянным, что забыл файлы дома. Но времени вернуться у меня уже нет. Не могли бы вы отправить мне копии?»

«Конечно, без проблем. Я сделаю копии, вы можете прийти прямо сейчас и забрать их».

«Здорово, но понимаете, я сейчас на другом конце города. Не могли бы вы отправить их мне по факсу?»

Это создало небольшую проблему, но вполне преодолимую. «У нас здесь нет факса», – ответила она. «Но факс есть в офисе этажом ниже. Думаю, они позволят мне воспользоваться им».

Он сказал: «давайте я позвоню в этот офис и попрошу их».

Леди в офисе ответила, что может помочь, но ей бы хотелось знать, кто за это заплатит. Ей нужен был номер счета.

«Я узнаю номер счета и перезвоню вам», – ответил он.

Затем он снова позвонил в адвокатскую контору, представился полицейским и просто спросил секретаря номер счета данного офиса. Без малейшего сомнения ему ответили.

Звоня обратно в офис, чтобы предоставить номер счета, он попутно извинился перед леди, которой пришлось спускаться этажом ниже, чтобы отправить ему факс.

Заметка

Откуда социальный инженер знает детали многих операций-полицейских департаментов, офисов прокуратуры, деятельности телефонных компаний, специфических организаций, чья деятельность связана с телекоммуникациями и компьютерами, и может помочь в его атаках? Потому что его работа-знать это. Такие знания – товар социального инженера, так как являются оружием в достижении цели.

Сокрытие его пути

Артуро также предстояло предпринять еще пару шагов. Всегда была возможность, что кто-нибудь все разнюхает и, приехав в магазин, столкнется с парочкой копов, которые обнаружат свое присутствие лишь тогда, когда кто-нибудь попробует узнать про пришедший факс. Он выждал немного и затем вновь позвонил в офис, чтобы убедиться, что леди отправила факс.

Затем он позвонил в другой магазин и использовал уловку по теме «как он благодарен за предоста-

вление работы и ему хочется написать благодарственное письмо менеджеру, которого, кстати, как зовут?» С этим маленьким кусочком информации он позвонил в первый магазин и сказал, что ему необходимо переговорить с их менеджером. Когда на другом конце провода подняли трубку, Артуро сказал: "здравствуйте, это Эдвард из магазина на 628 в Хартфильде. Мой менеджер, Анна сказала позвонить вам. У нас есть клиент, который чрезвычайно расстроен – кто-то дал ему факс не того магазина. Он здесь, ждет очень важного факса, который по ошибке был направлен в ваш магазин. "Менеджер пообещал найти этот факс и отправить в магазин в Хартфильде сразу же.

Артуро уже ждал во втором магазине, когда факс пришел туда. Заполучив копии, он позвонил леди из офиса и поблагодарил ее, добавив, что эти копии необязательно возвращать, их можно выкинуть. Затем он позвонил менеджеру первого магазина и также попросил его выкинуть копии факса. Таким образом, не осталось улик о его деятельности, кроме разговоров. Социальные инженеры знают, что безопасность никогда не бывает лишней.

Действуя в данном направлении, Артуро даже не пришлось платить денег за получение факса, и даже если бы полиция появилась в первом магазине, у него уже были на руках копии, и к тому времени он бы уже был вне пределов их досягаемости.

Конец этой истории: показание присяжного и предупреждение показали, что полиции было хорошо известно о деятельности Артуро. Это то, что ему следовало знать. К полуночи он пересек границу штата. Артуро был на пути к новой жизни, готовый начать свою деятельность заново.

Анализ обмана

Люди, которые напрямую работают в каких-либо поверенных офисах, в любом случае, находятся в прямом контакте с исполнителями закона – отвечают на вопросы, делают договоренности, получают сообщения. Кто-нибудь достаточно храбрый, чтобы назваться полицейским, представителем шерифа или кем-то еще, может добиться многого. Разумеется, если он не владеет терминологией или спотыкается через каждое слово от страха, никто не ответит на его запрос.

Сообщение от Митника

Вся правда заключается в том, что никто не застрахован от обмана со стороны социального инженера. Из-за темпа нашей повседневной жизни нам не хватает времени, чтобы задуматься над принятием какого-то решения, даже очень важного для нас. Запутанные ситуации, нехватка времени, эмоциональное напряжение могут очень легко сбить нас с толку. Таким образом, мы принимаем решение в спешке, не анализируя полученную информацию, такой процесс называется автоматическим ответом. Это работает и с госу-

дарственными, городскими и местными представителями закона. Мы все-люди.

Получение необходимого дебетного кода было решено с помощью обыкновенного телефонного звонка. Затем Артуро сыграл на симпатии собеседника с помощью карты а-ля «через 15 минут у меня встреча по этому делу». И я был настолько рассеянным, что забыл файлы дома. Но времени вернуться у меня уже нет. " Она действительно пожалела его и решила помочь.

Затем, используя не один, а два магазина, Артуро обезопасил себя от ареста во время получения факса. Существуют и другие способы затруднения отслеживания факса: вместо отправки его в другой магазин, атакующий может дать номер, который будет похож на номер факса, но на самом деле будет являться номером бесплатного интернет – сервиса, который при получении факса для вас, автоматически перешлет его на ваш е-мэйл. Таким образом, он может быть скачан прямо на компьютер атакующего, который нигде не засветится, и в будущем у него не возникнет проблем. К тому же, адрес е-мэйл или электронный номер факса могут быть уничтожены, как только задание будет выполнено.

Переводя стрелки

Молодой человек, которого я назову Майклом Паркером, был из тех людей, которые соображают немного поздно, что хорошо оплачиваемая работа достается обычно людям, окончившим колледж. У него был шанс поступить в местный колледж с получением частичной стипендии и займа на обучение, но это значило работать ночами и выходными, чтобы платить за аренду, еду, газ и авто страховку. Майкл, который всегда любил находить короткие пути решения проблемы, подумал, что, возможно, существует другой путь, который позволит быстрее выплатить долг и затратить меньше усилий. Дело в том, что он занимался изучением компьютеров с десяти лет и находил заманчивым изучать их работу, так что он решил посмотреть, может ли он создать себе ускоренный диплом бакалавра компьютерных наук.

Получение диплома без почета

Он мог вломиться в компьютерную систему государственного университета, найти записи того, кто получил диплом с оценками «хорошо» и «отлично», скопировать их, вписать свое имя и добавить в записи выпускников того года. Обдумывая эту идею, он понял, что существуют и другие записи и студентах, прожива-

ющих в кампусе, их платежах. И создавая записи лишь о прослушанных курсах и классах, можно сильно проколоться.

Составляя план дальше, он понял, что может достичь своей цели, посмотрев, нет ли выпускников с его фамилией, получивших степень компьютерных наук в соответствующий отрезок времени. Если так, можно лишь изменить личный социальный номер на рабочих формах; любая компания, проверяющая его имя и личный социальный номер, увидит, что он действительно владеет указанным званием (это не понятно большинству людей, но очевидно для него, что если он укажет один социальный номер на заявлении о приеме на работу и затем, если его наймут, укажет свой реальный. Большинство компаний никогда не проверяют, чей номер указал нанимающийся).

Включаясь к проблеме

Как найти Майкла Паркера в университетских записях? Он представлял себе это так: пойти в главную библиотеку в университетском кампусе, сесть за компьютерный терминал, выйти в интернет и получить доступ к сайту университета. Затем он позвонил в регистрационный офис. С ответившим человеком он провел стандартную для социального инженера беседу: «Я звоню из компьютерного центра, мы меняем конфигурацию сети и хотим убедиться, что не нарушили ваш доступ. К какому серверу вы подключаетесь?»

«Что значит сервер?» – спросили его.

«К какому компьютеру вы присоединяетесь, когда хотите получить академическую информацию о студентах?»

Ответ admin.rnu.edu дал ему имя компьютера, в котором хранились записи о студентах. Это был первый кусочек головоломки. Теперь он знал свою цель.

LINGO:

Dumb terminal -"немой терминал". терминал, который не содержит свой микропроцессор. Такие терминалы могут принимать лишь простые команды и отображать буквы и цифры

Он впечатал тот URL и не получил ответа – как и ожидалось, там стоял файрвол, блокирующий доступ. Он запустил программу, отображающую наличие сервисов, которые он мог запустить на удаленном компьютере и нашел открытый порт телнета, который позволял компьютеру удаленно присоединиться к другому компьютеру и получить к нему доступ, так как можно было использовать *dumb terminal* . Все, что ему нужно было знать, чтобы получить доступ-это обычный логин пользователя и пароль.

Он еще раз позвонил в регистрационный офис, прислушиваясь внимательно, чтобы убедиться, что разговаривает с другим человеком. Ему ответила женщина, и он опять представился работником компьютерного центра. Он сказал, что они установили новый про-

дукт для хранения административных записей и просит, чтобы она присоединилась к новой системе, которая все еще в стадии теста, чтобы проверить, правильно ли она работает. Он дал ей IP-адрес и провел через весь процесс.

Фактически, IP —адрес принадлежал компьютеру Майкла в библиотеке кампуса. Используя вышеназванный в этой главе процесс, он создал симулятор программы – ловушки, чтобы узнать под каким логином и паролем она заходит в систему студенческих записей. «Не работает», – ответила она. «Выдается сообщение, что логин неверен».

К этому моменту, симулятор передал символы имени ее аккаунта и пароля на терминал Майкла; миссия выполнена. Он ответил ей, что некоторые аккаунты еще не перенесены на эту машину. Но сейчас он внесет ее аккаунт и перезвонит ей. Очень внимательный к сокрытию следов, как и всякий опытный социальный инженер, он мог уточнить, что перезвонит позже, чтобы сказать, что тестовая система плохо работает, но если все будет хорошо, то ей перезвонят.

Полезный секретарь

Теперь Майкл знал, к какой системе необходимо получить доступ, имел логин и пароль. Но какими командами ему надо пользоваться, чтобы найти файлы с необходимой информацией, верным именем и датой? Студенческая база данных явно отвечает специфиче-

ским требованиям регистрационного офиса и имеет особый путь доступа к информации.

Первым шагом в решении этой проблемы было найти человека, который провел бы его через все ужасы поиска студенческой базы данных. Он вновь позвонил в регистрационный офис, опять выйдя на другого человека. Сказав, что звонит из деканата факультета инжиниринга, он спросил у женщины, кто бы мог помочь ему, так как возникли некоторые проблемы с доступом к студенческим академическим записям.

Немного позже он уже разговаривал с администратором базы данных и успешно играл на его симпатиях.

"Меня зовут Марк Селлерс, из офиса регистрации. Вы чувствуете ко мне жалость, да? Извините за звонок, но дело в том, что все старшие на совещании и вокруг нет никого, кто бы мог помочь мне. Мне необходимо восстановить список выпускников со степенью бакалавра компьютерных наук в период между 1990 и 2000 годами. Он нужен им к концу дня, но у меня он отсутствует, а я так долго стремился получить эту работу. Не будете ли вы так добры помочь парню, попавшему в беду? "Помогать людям, попавшим в беду было тем, что обычно делал администратор базы данных, и он терпеливо объяснил Майклу каждый шаг.

К тому времени, как они закончили разговор, Майкл загрузил вводный лист выпускников с необходимым дипломом за те года. Через несколько минут он обна-

ружил двух Майклов Паркеров, выбрал одного из них и получил его личный социальный номер, как и другую информацию, хранящуюся в базе данных.

Он только что стал Майклом Паркером, получившим звание бакалавра компьютерных наук в 1998 году.

Анализ обмана

Атакующий использовал одну уловку, о которой я раньше не упоминал: Атакующий попросил администратора провести его через весь процесс шаг за шагом. Достаточно сильное и эффективное действо, аналогичное тому, как если бы вы попросили владельца магазина помочь вынести вам предметы, которые вы только что из него украли.

Сообщение от Митника

Пользователи компьютера даже не подозревают о наличии угроз и уязвимостей, связанных с социальным инжинирингом, который существует в нашем мире высоких технологий. Они имеют доступ к информации, не разбираясь в деталях работы, не осознавая важности некоторых мелочей. Социальный инженер выберет своей целью работника с низким уровнем владения компьютером.

Предупреждение обмана

Симпатия, вина и запугивание-это три очень популярных психологических трюка, используемых социальным инженером, и вышеперечисленные истории продемонстрировали тактику действий. Но что можете сделать вы и ваша компания, чтобы избежать данных типов атак?

Защита информации

Некоторые истории в этой главе показывают опасность отправки файла кому-то незнакомому, даже человеку, который представляется работником вашей компании, а файл отправляется по *внутренней сети* на е-мэйл или факс.

Службе безопасности компании необходимо выстроить схему, обеспечивающую безопасность при пересылке важной информации какому-то незнакомому лично отправителю. Особые процедуры должны быть разработаны для передачи файлов с важной информацией. Когда запрос поступает от незнакомого человека, должны быть предприняты шаги к подтверждению его личности. Также должны быть установлены различные уровни доступа к информации.

Вот некоторые способы, которые следует обдумать:

Установите, насколько необходимо спрашивающе-

му это знать (что может потребовать получения одобрения со стороны владельца информации)

Храните логи всех транзакций

Утвердите список людей, которые специально обучены процедурам передачи информации и которым вы доверяете отправку важной информации. Требуйте, чтобы лишь эти люди имели право отсылать информацию за пределы рабочей группы.

Если запрос на информацию пришел в письменном виде (е-мэйл, факс или почта), предпримите особые шаги, чтобы убедиться в верности указываемого источника.

О паролях

Все сотрудники, которые имеют доступ к важной информации, а в наше время это все, кто имеют доступ к компьютеру, должны понимать, что даже такая простая процедура, как смена пароля, может привести к серьезной бреши в безопасности системы.

Занятия по безопасности должны включать в себя тему паролей и быть сфокусированы на процессе смены пароля, установки приемлемого пароля и опасностях, связанных с участием посторонних в этом. Занятия должны научить сотрудников подозрительно относиться к *любому* запросу по поводу их пароля.

Заметка

Именно на паролях сосредоточены атаки социальных инженеров, которые мы рассмотрели в отдельной

секции в главе 16, где вы также найдете особые рекомендации по данной теме.

Группа по отчетам

Ваша служба безопасности должна предоставить человека или группу, сформированную, как орган, в который поступали бы отчеты о подозрительной деятельности, направленной на атаку вашей организации. Все рабочие должны знать, куда обратиться в случае подозрения на электронное или физическое вторжение. Телефонный номер такого места всегда должен быть на виду, чтобы служащим не приходилось разгребать кучи бумаг в поисках его, во время попытки атаки.

Защитите вашу сеть

Служащие должны осознавать, что имя сервера или компьютера в сети это не пустяковая информация, а важная настолько, что может дать атакующему знание своей цели.

В частности, люди, такие как администраторы баз данных, которые работают с программным обеспечением, принадлежат к категории людей, которые располагают технической информацией, так что они должны работать в условиях жестких правил, устанавливающих личность человека, обратившегося к ним за советом или информацией.

Люди, которые регулярно предоставляют помощь в компьютерной сфере, должны отлично распознавать запросы, на которые нельзя ни в коем случае отвечать,

понимая, что это может быть атакой социального инженера.

Намного хуже осознавать, что в вышеупомянутой ситуации, атакующий подпадал под критерий законности: он звонил из кампуса, находился на сайте, требующем знание логина и пароля. Это лишь подтверждает необходимость наличия стандартной процедуры идентификации любого, запрашивающего информацию, особенно в данном случае, когда звонящий просил помощи в доступе к конфиденциальной информации.

Все эти советы особенно важны для колледжей и университетов. Ни для кого не новость, что хакинг – любимое времяпровождение для многих студентов, и также не секрет, что очень часто факультетские записи бывают целью их атак. Угрозы взлома стали настолько серьезны, что многие компании считают кампусы неким источником зла и добавляют в файрвол правило, блокирующее доступ с компьютеров, имеющих адрес **.edu*

Короче говоря, все студенческие и персональные записи любого характера должны рассматриваться как возможные цели для атак и быть хорошо защищены.

Тренировочные советы

Большинство атак такого плана очень просто отразить для человека, знающего, чего ожидать.

Для корпораций необходимо проведение фундамен-

тальной подготовки к такого рода ситуациям, но существует также необходимость *напоминать* людям об их знаниях.

Используйте яркие заставки, которые будут появляться при включении компьютера и содержать новый совет по безопасности каждый раз. Сообщение должно быть сделано таким образом, чтобы оно не исчезало автоматически, но требовало от пользователя нажатия на совет, который он / она только что прочитали.

Другой подход, который я могу посоветовать – это начать серию напоминаний о безопасности. Частые сообщения с напоминаниями очень важны; информирующие программы не должны иметь конца, сообщения должны иметь каждый раз разное содержание. Занятия показали, что такие сообщения более эффективны, когда написаны по-разному или используются различные примеры в них.

Еще один отличный способ – использовать короткие аннотации. Это не должна быть полная колонка, посвященная предмету. Лучше сделать пару-тройку маленьких колонок, как маленький экран в вашей собственной газете. В каждом случае такого письма представляйте очередное напоминание в коротком, хорошо запоминающемся виде.

Глава 9: Ответный удар

Перевод: Vedmak (wizard@mail.ru)

The String , упомянутый где-либо в этой книге (и, по моему мнению, самый лучший фильм, когда-либо снятый о мошенничестве), изображает ловкую задумку в массе обворожительных деталей. Операция, описанная в фильме – удачный пример того, как лучшие мошенники проделывают «the wire,» один из трех видов обманов, которых называют «большими мошенничествами». Если вы хотите знать, как команда профессионалов проделывает аферу, загребая большое количество денег за один вечер, что лучшего учебника не найти.

Но обычные мошенники, со всеми их специфическими уловками, в целом действуют по определенной схеме. Иногда уловка работает в обратном направлении, что и называется *«обратный обман».* Трюк в том, что злоумышленник организует ситуацию так, что жертва просит *его* о помощи, либо злоумышленник отвечает на просьбу коллеги. Как это работает? Сейчас Вы это узнаете.

LINGO

ОБратный обман Мошенничество, в котором жертвы сама просит мошенника о помощи.

Исскуство дружелюбного убеждения

Когда среднестатистический пользователь воображает компьютерного хакера, на ум обычно приходит нелестный образ одинокого, замкнутого умника, лучший друг которого – компьютер и которому трудно общаться средствами, отличными от IM. Социальный инженер, кстати, часто обладающий определенными навыками взлома, имеет массу коммуникативных качеств и развитые способности для использования и манипулирования людьми. Это позволяет ему получать необходимую информацию способами, о возможности которых Вы даже не подозреваете.

ЗвонокАнжеле

Место: valley branch, industrial federal bank.

Время: 11:27

Анжела Висновски ответила на телефонный звонок человека, который вот-вот должен был получить приличное наследство и интересовался различными вариантами накопительных вкладов, депозитных сертификатов и других вариантов инвестирования, которые она могла бы ему порекомендовать как надежные, но приносящие определенный доход. Она обяснила, что существует достаточно много вариантов и спросила,

не будет ли лучше ему подъехать и на месте обсудить их. Человек ответил, что сразу по получении отправляется в командировку и запланировал еще массу мероприятий. Поэтому она начала рекомендовать некоторые из возможностей, сообщая размеры процентных ставок, что будет, если продать CD (имхо какой-то специальный банковский термин) раньше и т.д., попутно пытаясь определить предполагаемые цели инвестиций.

Ей даже удалось достигнуть определенных успехов в этом вопросе, когда он сказал: «О, простите, мне нужно ответить на другой звонок. Когда я смогу закончить этот разговор и принять решение? Когда у Вас обед?». Она ответила ему 12:30 и он обещал позвонить до обеда или на следующий день.

Звонок Льюису

Крупные банки используют защитные коды для внутреннего пользования, которые меняются каждый день. Когда кому-то из сотрудников требуется информация из другого подразделения, он подтверждает свои права на информацию называя код дня. Для дополнительной защиты некоторые банки используют несколько кодов каждый день. На Западном Берегу в вышеупомянутом Industrial Federal Bank каждый сотрудник получает список из пяти кодов (обозначаемых А – Е) на своем компьютере каждое утро.

Место: то же

Время: 12:48 того же дня

Льюис Халпберн (Louis Halpburn) работал как ни в чем ни бывало, когда днем раздался телефонный звонок. Обычный звонок, один из тех, на которые он регулярно отвечал несколько раз в неделю.

– Здравствуйте, – сказал звонивший. – Это Нэйл Вебстер (Neil Webster). Я звоню из отделения 3182, это в Бостоне. Будьте добры Анжелу Висновски.

– Она обедает. Я могу помочь?

– Да, она оставила сообщение с просьбой прислать факсом информацию по одному из наших клиентов.

Казалось у звонившего был не самый удачный день.

– Обычно этим занимается другой человек, который сейчас заболел, – сказал он, – я уже совсем замотался с этим, уже 4 часа, а у меня назначен прием у врача через полчаса.

Тонкость в том, что рассказывая о причинах, вызывающих сочувствие у собеседника, злоумышленник как бы смягчает свою просьбу. Он продолжил:

– Кто-то принял ее звонок, номер факса записан неразборчиво… 213.. что-то там… Что там дальше?

Льюис назвал номер и звонивший сказал:

– ОК, спасибо. Но перед тем, как послать Вам факс, я должен знать код В.

– Но это ВЫ мне позвонили, – сказал Льюис достаточно холодно, чтобы человек из Бостона понял, что он имеет ввиду.

Это неплохо, подумал звонивший. *Это даже хорошо, что люди не падают от одного вежливого пинка. Если бы они перестали хоть немного сопротивляться, работа бы стала совсем легкой, и я бы вконец обленился.*

Льюису он сказал:

– Наш начальник отделения просто параноик, когда дело касается подтверждения полномочий при отсылке чего-либо куда либо. Но, послушайте, если Вам не особо нужна эта информация, я могу ничего не посылать. И не надо ничего подтверждать.

– Слушайте, – сказал Льюис, – Анжела вернется примерно через полчаса. Я могу сказать ей Вам перезвонить.

– Ладно, я просто скажу ей, что не мог послать информацию сегодня, потому что Вы не подтвердили законность этого запроса кодом. Если я не заболею завтра, я ей позвоню…

Хм… Сообщение помечено как «Срочное»… Ну да ладно, в любом случае без подтверждения у меня связаны руки. Вы ведь скажете ей , что я пытался послать, но вы не назвали код, хорошо?

Льюис оказался под давлением. Отчетливый признак раздражения слышался в голосе из телефонной трубки.

– Хорошо, – сказал он. – Минуту, мне нужно подойти к компьютеру. Какой Вам нужен код?

– B (читается ‘би’ – прим. переводчика), – сказал собеседник.

Он отложил трубку и вскоре взял ее снова. «3184»

– Это неправильный код.

– Нет, правильный: код B – 3184.

– Я не говорил B, я сказал «E» (читается ‘и’ – прим. переводчика).

– Черт. Минуту…

– E – 9697.

– 9697, да, все правильно. Я отправляю факс, ок?

– Да… конечно.. спасибо.

Звонок Уолтеру

– Государственный индустриальный банк, это Уолтер.

– Привет, Уолтер, это Боб Грабовски (Bob Grabowski), Студио Сити (Studio City), 38-е отделение, мне нужно, чтобы Вы нашли образец подписи клиента. Образец подписи – это больше, чем просто подпись клиента, карточка содержит также удостоверяющую информацию вроде номера социального страхования, даты рождения, девичьейфамилии матери, иногда даже номер водительского удостоверения. Вообще очень полезная вещь для социального инженера.

– Да не вопрос. Какой код C?

– За моим компьютером сейчас другой сотрудник, – сказал звонивший, – Но я только что называл коды B и

Е, и помню их так. Спроси меня один из них?

– Ок, код Е?

– Е – 9697.

Через несколько минут Уолтер отправил по факсу образец подписи по запросу.

Звонок Донне Плейс

– Здравствуйте, это мр. Ансельмо.

– Чем я могу Вам помочь на этот раз?

– Какой номер на 800 мне надо набрать, когда я хочу проверить кредитован ли уже вклад?

– Вы клиент банка?

– Да, я долго не пользовался номером и теперь забыл, где он записан.

– Номер 800-555-8600.

История Винса Капели

Сын уличного полицейского из Спокана (США, штат Вашингтон – прим. переводчика) Винс с ранних лет знал, что не собирается надрываться часами и рисковать своей шеей за маленькие деньги. Двумя принципиальными целями его жизни стало: уехать из Спокана и начать работать на себя. Когда он учился в старших классах, усмешки его знакомых только раззадорили его еще больше – они думали, что это невероятно смешно, что он так хочет открыть дело, но не знает какое.

В глубине души Винс знал, что они правы. Единственное, что у него получалось хорошо, – это играть

принимающим в школьной бейсбольной команде. Но не настолько хорошо, чтобы получать стипендию и совсем нехорошо для профессионального бейсбола. Какой бизнес он мог бы начать?

И только одного никогда не понимали одногруппники Винса: Если у кого-то из них что-то было, скажем новый складной нож, модные теплые перчатки или новая симпатичная подружка, если это нравилось Винсу, вскоре он это получал. Нет, он не крал ничего за чьей-либо спиной, этого не требовалось. Владелец сам охотно отказывался и потом удивлялся, как такое могло произойти. Не помогали даже расспросы самого Винса: Он сам не знал, как это получается. Люди, казалось, разрешали ему все, что он хотел.

Винс Капели был социальным инженером с ранних лет, даже никогда не слышав этого термина.

Его друзья разом перестали смеяться, когда все они получили по диплому. Пока другие слонялись по городу в поисках работы, на которой не надо было говорить «Не желаете ли картошку-фри?» отец Винса отослал его к старому полицейскому, который уволился со службы, чтобы открыть свое частное детективное агентство в Сан-Франциско. Тот быстро увидел талант Винса и взял его на работу.

Это было 6 лет назад. Он ненавидел работу, заключавшуюся в сборе компромата на неверных супругов, которая превращалась в мучительные часы тупого си-

дения и наблюдения, но чувствовал постоянный интерес к заданиям раскопать информацию о капиталах для адвокатов, пытающихся выяснить, что жалкий нищий достаточно богат и стоит подачи иска.

Как, например, когда ему требовалось заглянуть в банковские счета парня по имени Джо Марковиц (Joe Markowitz). Джо, вероятно, провернул темное дельце с своим бывшим другом и это друг теперь хотел знать, был ли Марковиц достаточно богат, чтобы в случае подачи иска вернуть с него некоторую сумму денег.

Для начала Винсу желательно было бы узнать по меньшей мере один, но лучше два, банковских защитных кода на текущий день. Это звучит почти нереально, что может заставить банковского работника открыть лазейку в собственной системе безопасности? Спросите себя, если бы вам потребовалось что-нибудь подобное, как бы вы этого добились?

Для людей вроде Винса это очень просто.

Люди доверяют тебе, если ты знаешь их профессиональный жаргон, некую внутреннюю форму общения их компании, скрытую от посторонних глаз. Это как бы способ показать, что ты один из них, своего рода секретное рукопожатие.

Мне не требовалось знать много для подобной операции. Уж точно не операция на мозге. Для начала потребовался лишь номер отделения банка. Когда я позвонил в отделение на Бикэн Стрит (Beacon Street)

в Буффало, человек, который ответил, был похож на болтуна.

– Это Тим Экерман, – сказал я. Подойдет любое имя, он, очевидно, не собирался его никуда записывать. – Какой у Вас номер отделения?

Он хотел знать, назвать ли “телефон или номер отдела”, что довольно-таки глупо, потому что я только что набрал номер, не так ли? (скорее всего, это своеобразная процедура аутентификации на фирме – прим. Редактора)

“Номер отдела” – 3182, – ответил он. Вот так. Никаких там, «Зачем Вам это надо?» и т.п. Потому что это не секретная информация, это написано почти на каждом кусочке бумаги, с которым они работают.

Шаг второй: позвонить в отделение, где обслуживается моя цель, получить имя одного из их сотрудников и выяснить, кто из них будет отсутствовать во время обеда. Анжела. Уходит в 12:30. Все путём!

Шаг третий: звоним в то же отделение, пока Анжела обедает, говорим, что мы из отделения такого-то из Бостона, Анжеле нужна информация по факсу, давайте нам код дня. Это самая сложная часть. Если бы я придумывал тест для социального инженера, я бы обязательно включил бы в него что-нибудь подобное, когда твоя жертва становится подозрительной – и не без оснований – и ты продолжаешь давить пока не сломаешь ее и не получишь нужную информацию. Вы не

сможете сделать это, повторяя строчки сценария или заучив процедуру, необходимо прочитать свою жертву, понять ее настроение, играть с ней, как с рыбкой, отпуская немного, а затем вновь подтягивая леску. И так пока не поймаешь ее в сеть, и она не шлепнется в лодку. Шлеп!

Итак, я его поймал и заполучил один из кодов дня. Это успех. Большинство банков используют один код, так что я уже мог бежать домой. Промышленный банк использует пять кодов, так что иметь один код из пяти маловато. С двумя из пяти у меня были бы существенно большие шансы пройти следующий эпизод этого маленького спектакля. Мне понравилась фишка про «Я не сказал ‘би’, я сказал ‘и’». Когда это срабатывает, это прекрасно. А срабатывает это в большинстве случаев.

Получить третий код было бы еще лучше. Причем у меня действительно получалось получить их за один звонок – ‘B’, ‘D’ и ‘E’ так похоже звучат, что вы можете настаивать на том, что вас снова не поняли. Но это только в разговоре с действительно слабым противником, а этот человек легкой добычей не был. Я ушел с двумя.

Коды дня станут моим ключом к получению образца подписи. Я звоню, а человек спрашивает код C. Но у меня только B и E. Но это совершенно не конец света. Необходимо оставаться хладнокровным в такие мо-

менты, говорить уверенно, продолжать максимально ровно, я сыграл что-то типа: «Мой компьютер сейчас занят, спросите меня один из этих кодов».

Мы все сотрудники одной компании, мы все делаем одно дело, надо помочь напарнику – так, надо надеяться, думает жертва в этот момент. И он играл прямо по сценарию. Он выбрал вариант из предложенных, я дал ему правильный ответ, он отправил мне факс с образцом подписи.

Почти у цели. Еще один звонок дал мне номер телефона, по которому автоматическая служба зачитывает клиенту требуемую информацию. Из карточки с образцом подписи, я знал все номера счетов жертвы и его PIN-код, т.к. банк использует первые пять или последние 4 цифры номера карточки социального страхования. Итак, с ручкой в руках, я позвонил в службу и после нескольких минут и пары нажатий на кнопки я получил последние сведения о балансе на всех счетах, и плюс к этому – его последние депозиты и съемы средств по ним.

Все, что заказывал мой клиент и даже больше. Я всегда люблю дать немножко больше, чем требуется за те же деньги. Клиент должен быть счастлив. Кроме того, повторяемость бизнеса – это основа развития.

Анализируя обман

Ключевым моментов всего этого эпизода было получение всех необходимых кодов дня, и для достиже-

ния этого, атакующий, т.е. Винс использовал несколько различных приемов.

Он начал с небольшого словесного «выкручивания рук», когда Льюис отказался дать ему код. Льюис был прав в своей подозрительности – коды придуманы для того, что бы использовать их в противоположном направлении. Он знал, что при обычном порядке неизвестный звонящий сообщит ему защитный код. Это был критический момент для Винса, от этого зависел успех всей задуманной им операции.

Столкнувшись с подозрительностью Льюиса, Винс просто сгладил ее, вызывая симпатию («собирался к доктору»), используя давление (“мне уже надоело всем этим заниматься, уже 4 часа») и манипулирование («Скажите ей, что не дали мне код»). На самом деле, Винс не угрожал ему, он только подразумевал это: «Если вы не дадите мне защитный код, я не вышлю информацию о клиенте, которую просил ваш коллега, и я скажу ему, что собирался послать, но вы не согласились сотрудничать».

Не будем, однако, поспешно винить Льюиса. В конце концов, человек, звонивший по телефону знал (или по крайней мере похоже, что знал), что Анжела запрашивала факс. Звонивший знал о защитных кодах, и знал, что они называются буквами алфавита. Он сказал, что начальник его отделения требует их для большей защищенности. На самом деле нет причин не дать ему

подтверждение, о котором он просит.

Льюис не одинок. Сотрудники банков сообщают защитные коды социальным инженерам каждый день. Невероятно, но факт.

Существует грань, за которой действия частного детектива перестают быть законными и становятся преступными. Винс не нарушил закон, когда он узнал номер отделения. Он даже не нарушил закон, когда обманом заставил Льюиса выдать ему два защитных кода. Он перешел грань, когда получил по факсу конфиденциальную информацию о клиенте банка.

Но для Винса и его нанимателя это не слишком рискованное преступление. Когда Вы воруете деньги или вещи, кто-то замечает, что они пропали. Если Вы украли информацию, часто никто этого не заметит, так как информация по прежнему остается у владельца.

Сообщение Митника

Устные защитные коды эквивалентны паролям в обеспечении удобных и надежных средств защиты информации. Но сотрудники должны быть осведомлены об уловках, применяемых социальными инженерами, и обучены не выдавать ключи от королевства.

Полицейские – жертвы обмана

Для не слишком чистого на руку частного детектива или социального инженера часто бывает весьма сподручно знать номер чьего-нибудь водительского удостоверения, например, если необходимо притворить-

ся другим человеком с целью получения информации о его банковских счетах.

Исключая кражу бумажника или подсматривание через плечо при удобной возможности, выяснение номера водительского удостоверения представляется практически невозможным. Но для любого человека даже с самыми скромными навыками в социальной инженерии это вряд ли проблема. Конкретному социальному инженеру – назовем его Эрик Мантини (Eric Mantini), необходимо было регулярно узнавать номер удостоверений и регистрационные номера транспортных средств. Эрик понимал, что бессмысленно раз за разом рисковать, звоня в Управление Транспорта (Department of Motor Vehicles, DMV) и используя всяческие ухищрения всякий раз, когда ему нужна подобная информация. Он захотел выяснить, а нет ли способа упростить процесс.

Возможно, никто не думал об это прежде, но он нашел способ получать информацию в мгновение ока, когда она требовалась. Он сделал это воспользовавшись преимуществами услуги, предоставляемой Управлением Транспорта (УТ) его штата. Многие УТ (или аналогичное управление в вашем штате) делают секретную информацию о гражданах доступной страховым компаниям, частным детективам и некоторым другим лицам, которые законодательный орган штата считает в праве пользоваться ей для пользы экономиче-

ской и социальной жизни в целом.

УТ, конечно, имеет соответствующие ограничения на типы информации, которую можно предоставлять. Страховщики могут иметь доступ к определенным типам информации из досье, но не ко всем. Различные ограничения установлены для частных детективов и т.д.

Для сотрудников правоохранительных органов в основном применяется другое правило: УТ обеспечит любой информацией из архива любого блюстителя порядка, правильно подтвердившего свою личность. В штате, где жил Эрик для идентификации требовался Код Запрашивающего (Requestor Code), назначаемый УТ, и номер водительского удостоверения. Сотрудник Управления должен был всегда сверять имя офицера с его номером водительского удостоверения и еще какой-то информацией – обычно датой рождения – перед передачей какой-либо информации.

Социальный инженер Эрик захотел никак не меньше, как надеть маску полицейского! Как ему это удалось? С помощью обратного обмана полицейских!

Хитрость Эрика

Сначала он позвонил в справочную и спросил номер телефона центрального офиса Управления Транспорта в столице штата. Ему дали номер 503-555-5000. Естественно, это был номер для обычных звонков населения. Затем он позвонил в ближайший полицейский

участок и спросил номер телетайпной – откуда передавалась и где принималась информация от других правоохранительных органов, государственной базы данных о преступлениях, местных ордерах и постановлениях и т.п. Позвонив в телетайпную, он спросил номер телефона, по которому сотрудники должны звонить в управление транспорта.

– Вы кто? – спросил офицер из телетайпной.

– Это А1. Я набирал 503-555-5753, – ответил Эрик. Номер основывался частично на предположении, частично был взять с потолка: совершенно очевидно, что подразделение в УТ, отвечающее на звонки сотрудников правоохранительных органов будет иметь тот же код области, что и номер для публичных звонков; и практически наверняка следующие 3 цифры номера (префикс) тоже совпадут. И, по-хорошему, все что нужно – это выяснить последние 4 цифры.

В телетайпную не звонят «с улицы», а звонивший уже знал большую часть номера. Конечно, это был кто-то из сотрудников.

– Номер 503-555-6127, – сказал офицер.

Итак, Эрик теперь знал специальный телефонный номер управления транспорта для сотрудников правоохранительных органов. Но одного номера было недостаточно; отдел управления должен был иметь гораздо больше, чем одна телефонная линия и Эрику требовалось знать, сколько там линий и номер каждой из них.

Коммутатор

Чтобы осуществить задуманное, ему нужно было получить доступ к телефонному коммутатору, который управлял телефонной связью между полицией и УТ. Он позвонил на телефонный узел и представился сотрудником компании Нортел (Nortel), производителя DMS-100, одного из наиболее распространенных коммерческих телефонных коммутаторов. Эрик спросил:

– Не могли бы Вы переключить меня на техника, который обслуживает DMS-100?

Технику он сказал, что из Центра Поддержки Технических Специалистов Нортела в Техасе, и объяснил, что они создают базу данных для обновления всех коммутаторов свежими версиями ПО. Предполагается, что обновление будет происходить удаленно, без вмешательства техников. Но ему нужен входной номер дозвона на коммутатор, чтобы произвести обновление прямо из Центра Поддержки.

Все это звучало полностью правдоподобно, и техник дал Эрик номер. Теперь Эрик могу напрямую звонить на один из государственных телефонных коммутаторов.

Для предотвращения проникновения извне, коммерческие коммутаторы этого типа защищены паролем, как и любая корпоративная компьютерная сеть. Любой хороший социальный инженер с некоторой подготовкой в области фрикинга (phreaking) знает, что нор-

теловские коммутаторы имеют специальную учетную запись для обновления программного обеспечения: NTAS (Nortel Technical Assistance Support). Но каков пароль? Эрик звонил несколько раз, пробуя один из очевидных или часто используемых вариантов. Пароль NTAS не подошел… Также как и «helper», и «patch»…

Тогда он попробовал «update» … и он подошел. Типично. Использование очевидных, легко угадываемых паролей лишь слегка лучше, чем отсутствие пароля.

Полезно хорошо разбираться в своей сфере деятельности; Эрик, пожалуй, знал о коммутаторе и о том, как его программировать столько же, сколько хороший техник. Имея авторизированный доступ к коммутатору, он получил полный контроль над телефонными линиями, среди которых была его цель. Со своего компьютера, Эрик сделал на коммутаторе запрос по номеру телефона, выданного ему для звонков в УТ, 555-6127. Он обнаружил еще 19 других линий, расположенных в том же отделе. Очевидно, что там обрабатывают большой объем звонков.

Для каждого входящего звонка коммутатор был запрограммирован перебирать 20 телефонных линий до нахождения первой незанятой.

Он выбрал восемнадцатую по счету линию в последовательности и ввел код, который подключал переадресацию вызова для нее. В качестве номера для переадресации он ввел номер своего нового, дешевого,

заранее предоплаченного сотового телефона, из тех, что так любят драгдиллеры за дешевизну и, соответственно, возможность легко выкинуть, когда дело будет сделано.

С подключенной переадресацией на восемнадцатой линии, как только отдел будет достаточно занят, обрабатывая 17 звонков, следующий пришедший звонок не прозвонит в отделе управления транспорта, а будет переброшен на сотовый Эрика. И он приготовился ждать.

Звонок в управление

Незадолго до восьми утра зазвонил сотовый телефон. Это самая лучшая часть, просто прелесть. Здесь Эрик, соц. инженер, разговаривает с полицейским, человеком, наделенным властью прийти и арестовать его или получить ордер на обыск.

И даже не один коп, а несколько, один за другим. Однажды Эрик обедал в ресторане с друзьями, экспромтом отвечая на звонки примерно каждые пять минут, записывая информацию на бумажных салфетках. И он все еще находил это забавным.

Общение с полицейскими ничуть не беспокоит подготовленного соц. инженера. По сути, водить полицию за нос даже добавляло Эрику острых ощущений.

А звонки проходили примерно так:

– Управления транспорта, добрый день.

– Это детектив Андрю Коул (Andrew Cole).

– Здравствуйте, детектив. Чем я могу Вам помочь

сегодня?

«I need a Soundex on driver's license 005602789,» he might say, using the term familiar in law enforcement to ask for a photo-useful, for example, when officers are going out to arrest a suspect and want to know what he looks like.

«Sure, let me bring up the record,» Eric would say. «And, Detective Cole, what's your agency?»

«Jefferson County.» And then Eric would ask the hot questions:

"Detective, what's your requestor code?

What's your driver's license number. «What's your date of birth»

The caller would give his personal identifying information. Eric would go through some pretense of verifying the information, and then tell the caller that the identifying information had been confirmed, and ask for the details of what the caller wanted to find out from the DMV. He'd pretend to start looking up the name, with the caller able to hear the clicking of the keys, and then say something like, «Oh, damn, my computer just went down again. Sorry, detective, my computer has been on the blink, all week. Would you mind calling back and getting another clerk to help you?»

– Мне нужно Soundex по водительскому удостоверению 005602789, – мог спросить полицейский, используя знакомый правоохранительным органам термин.

Таким способом он заканчивал разговор, не вызы-

вая никаких подозрений по поводу того, что не смог обработать запрос офицера полиции. А между тем Эрик уже владел украденной личностью, которую мог использовать для получения конфиденциальной информации из управления в любое время.

Поговорив по телефону несколько часов и получив дюжину кодов запрашивающего, Эрик позвонил на коммутатор и отключил переадресацию звонков.

Многие месяцы после этого он получал денежные отчисления от законных частных детективных агентств, которым было все равно, как он добывал информацию. При необходимости Эрик звонил на коммутатор, включал переадресацию и собирал очередную пачку удостоверений личности полицейских.

Анализируя обман

Давайте взглянем еще раз на хитрости, с помощью которых Эрику удалось обмануть стольких людей. На первом шаге он заставил помощника шерифа в телетайпной ему конфиденциальный номер телефона управления транспорта совершеннейшему незнакомцу, принимая собеседника за свое без проверки его личности.

Затем кто-то на телефонном узле сделал то же самое, веря, что Эрик из компании-производителя оборудования, и сообщил ему номер телефона для дозвона прямо на коммутатор, обслуживающий управление транспорта.

Эрик имел широкие возможности для взлома коммутатора из-за слабой политики безопасности фирмы-производителя, которая использует одну и ту же сервисную учетную запись на всех своих коммутаторах. Для соц. инженера эта беспечность превращает процесс угадывания пароля в легкую прогулку, учитывая, что технический персонал, обслуживающий коммутатор, как, в общем-то, и все люди, выбирают пароли, которые им просто запомнить.

Имея доступ к коммутатору, он настроил переадресацию вызова для одной из телефонных линий управления транспорта на свой сотовый телефон.

И, наконец, в последней и самой ужасающей части истории, Эрик обманом заставлял одного офицера полиции за другим выдавать ему не только их код запрашивающего, но и персональную приватную информацию, знание которой позволило Эрику играть роль полицейского. Несмотря на необходимость обладать определенными техническими знаниями для того, чтобы справиться с задачей, вряд ли бы мошеннику удалось осуществить задуманное без помощи многих людей, у которых не возникло даже мысли о том, что они разговаривают с самозванцем.

Эта история – еще одна иллюстрация феномена, почему люди не спрашивают себя «Почему я?» Почему офицер из телетайпной предоставил информацию какому-то представителю шерифа, которого он не знал

или, в нашем случае, незнакомцу, выдающему себя за помощника шерифа, вместо того, чтобы посоветовать тому узнать телефон у напарника или собственного сержанта? И опять, единственное объяснение, которое приходит мне на ум, что люди редко задают себе этот вопрос. И с чего бы им задавать этот вопрос? А, может быть, они не хотят показаться проблемными или бесполезными? Дальше можно только строить догадки на этот счет. Но соц. инженеру не важно «почему», им важно лишь то, что эта маленькая деталь позволяет легко получить информацию, которую существенно сложнее добыть другими путями.

Сообщение Митника

Если в вашей компании используется телефонный коммутатор, что будет делать ответственный сотрудник, если ему позвонить производитель оборудования с просьбой сообщить номер для дозвона на коммутатор? И, кстати, этот сотрудник вообще когда-либо менял на коммутаторе пароль по умолчанию для служебной учетной записи? Этот пароль легко угадывается или подбирается по словарю?

Предотвратить обман

Грамотно используемый защитный код существенно повышает уровень безопасности. Неграмотно используемый защитный код может быть даже хуже, чем вообще отсутствие кода, так как он создает иллюзию защиты, которой на самом деле нет. Что хорошего в ко-

дах, если ваши сотрудники не хранят их в секрете?

Любой компании, использующий устные защитные коды, необходимо ясно и четко объяснить сотрудникам, когда и как эти коды используются. Правильно проинструктированный персонаж из первой части этой главы не должен был бы полагаться на свою интуицию, когда незнакомец спросил его про защитный код. Он почувствовал, что у него не должны спрашивать эту информацию в данной ситуации, но отсутствие четкой политики безопасности и хороший здравый смысл – и он сдался.

Инструкции по безопасности должны включать в себя описание действий служащего, получающего несанкционированный запрос защитного кода. Все сотрудники должны быть обучены немедленно сообщать обо всех запросах защитных кодов (таких как код дня или пароль), сделанных при необычных обстоятельствах. Они также должны сообщать обо всех неудачных попытках установить личность запрашивающего.

Наконец, служащий должен записывать фамилию звонившего, телефон и название офиса или подразделения, прежде чем повесить трубку. А до того, как перезвонить, он должен убедиться, что в указанной организации действительно имеется сотрудник с такой фамилией и что телефон, по которому надо перезвонить действительно телефон этой организации. В большинстве случаев это простая тактика – практически все,

что нужно, чтобы убедиться, что звонящий на самом деле тот, за кого себя выдает.

Проверка становится несколько сложнее, когда у компании есть только напечатанный телефонный справочник вместе с электронной онлайновой версии. Люди нанимаются, люди увольняются, они переходят из отдела в отдел, меняют должности и телефоны. Твердая копия телефонного справочника устаревает в день публикации, еще даже до распространения. И даже электронным справочникам нельзя доверять, потому что соц. инженеры знают, как их подделать. Если сотрудник не может проверить номер телефона по независимому источнику, его необходимо проинструктировать о других способах сделать это, например, обратившись к старшему менеджеру.

Глава 11: Сочетая технологию и социальную инженерию

Перевод: Daughter of the Night (admin@mitnick.com.ru)

Социальный инженер живет своей возможностью манипулировать людьми, заставлять делать то, что поможет ему достичь своей цели, но успех обычно требует большого количества знаний и навыков в использовании компьютеров и телефонных систем.

Взлом решетки

Какие системы вы можете вспомнить, защищенные от взлома – физического, телекоммуникационного или электронного? Форт Нокс ? Конечно. Белый Дом? Абсолютно точно. NORAD (North American Air Defence), Северно-американская воздушно-защитная база, расположенная глубоко под горой? Определенно.

А как насчет тюрем и мест заключений? Они должны быть не менее безопасны, чем другие места в стране, верно? Люди редко убегают, и даже если это им удается, их обычно вскоре ловят. Вы можете думать, что государственная организация будет неуязвима для атак социальных инженеров. Но вы будете не правы – нигде нет такой вещи, как «защита от дурака».

Несколько лет назад, пара профессиональных мошенников столкнулись с проблемой. Так получилось, что они унесли большую сумку наличных у местного судьи. У этой пары уже не первый год были проблемы с законом, но сейчас федеральные власти особо заинтересовались. Они поймали одного из мошенников, Чарльза Гондорффа, и посадили его в исправительную колонию рядом с Сан-Диего. Федеральный судья приказал удерживать его как угрозу обществу и потенциального беглеца.

Его друг Джонни Хукер знал, что для Чарли потребуется хороший адвокат. Но откуда взять деньги? Как и у многих других мошенников, все его деньги уходили на хорошую одежду, модные машины и женщин так же быстро, как и приходили. Джонни с трудом хватало денег на проживание.

Деньги на адвоката должны были прийти после очередного дела. Джонни не собирался делать все самостоятельно. Чарли Гондорфф всегда планировал все их аферы. Но Джонни даже не смел зайти в исправительную колонию, чтобы спросить у Чарли, что делать, учитывая то, что федералы знали, что в преступлениях участвовали двое, и жаждали заполучить второго. Только члены семьи могли посещать заключенных, что означало, что ему пришлось бы воспользоваться фальшивым удостоверением, утверждая, что он – член семьи. Пытаться использовать фальшивое удостоверение личности в федеральной тюрьме – не самая разумная идея.

Нет, ему надо было как-то связаться с Гондорффом.

Это будет нелегко. Ни одному заключенному из федеральной, штатной или местной организации не позволено отвечать на звонки. Над каждым телефоном в федеральной колонии висят таблички, на которой может быть написано, к примеру, «Предупреждаем вас, что все Ваши разговоры с этого телефона будут подвергнуты прослушиванию, и использование этого теле-

фона означает согласие с прослушиванием». Правительственные работники будут слушать ваши звонки, когда совершение преступления – это способ продления государственно-оплачиваемого отпуска.

Джонни знал, что некоторые звонки не прослушиваются: звонки между заключенным и его адвокатом – отношения, защищенные Конституцией, к примеру. Вообще то, учреждение, где задерживался Гондорфф, было соединено напрямую с Офисом Общественных Защитников (ООЗ). Поднимая один из телефонов, устанавливается прямое соединение с ООЗ. Телефонная компания называет это *прямой линией* . Ничего не подозревающая администрация полагает, что эта служба безопасна и неуязвима для вторжения, потому что исходящие звонки поступают только в ООЗ, а входящие звонки блокируются. Даже если кто-либо както узнает номер, он запрограммирован в телефонной компании на *deny terminate(запрет прекращения)* , неуклюжий термин телефонных компаний для услуги, где запрещены входящие звонки.

Поскольку любой достойный мошенник отлично разбирается в искусстве обмана, Джонни понял, что можно решить эту проблему. Изнутри, Гондорфф уже пытался поднимать трубку и говорить: «это Том, из ремонтного центра компании. Мы проверяем эту линию, и мне надо, чтобы вы набрали 9, а потом 00». Девятка открыла бы доступ на внешние линии, а ноль-ноль

бы соединили с оператором по дальним звонкам. Но это не сработало – человек, ответивший на вызов, уже знал этот трюк.

Джонни был более успешен. Он уже узнал, что в тюрьме есть десять жилых отделений, каждое с прямой линией к Офису Общественных Защитников. Джонни встретил несколько препятствий, но как социальный инженер, он знал, как преодолеть эти раздражающие камни преткновения. В каком именно отделении был Гондорфф? Какой был номер у службы прямого соединения с этим отделением? И как ему передать его первое сообщение Гондорффу, чтобы оно не было перехвачено тюремными властями?

То, что может показаться невозможным для среднестатистического человека, как получение секретных номеров, расположенных в государственных заведениях, – не более чем несколько звонков для афериста. После пары бессонных ночей мозговой атаки, Джонни проснулся однажды утром с полным планом в голове, состоящим из пяти пунктов.

Во-первых, надо узнать номера десяти отделений, соединенных с ООЗ.

Все 10 надо изменить на прием входящих вызовов.

Потом надо узнать, в каком отделении Гондорфф задерживается.

После этого надо выяснить, какой номер соединен с этим отделением.

И, наконец, договориться с Гондорффом о звонке так, чтобы правительство ничего не заподозрило.

Лакомый кусочек , подумал он.

LINGO

Прямое соединение – Термин телефонных компаний для телефонной линии, которая соединяется с определенным номером когда поднята трубка.

Deny Terminate – Сервис телефонной компании, где оборудование настроено так, что входящие звонки не могут быть приняты с определенного номера.

Звоню в Ma Bell (американская телеф. компания – прим. пер.)

Джонни начал со звонков в офис телефонной компании под видом сотрудника гособслуживания, организации, ответственной за приобретение товаров и услуг для правительства. Он сказал, что работает над заказом по покупке дополнительных услуг, и хотел получить счета по всем используемым прямым линиям связи, включая рабочие номера и телефонную стоимость в тюрьме Сан-Диего. Женщина была рада помочь.

Чтобы убедиться, он попробовал набрать один из номеров, и ответил типичный голос с записи: «Эта линия отключена или не обслуживается». На самом деле ничего подобного не имелось в виду, это означало, что линия запрограммирована блокировать входящие звонки, как он и ожидал.

Он знал из его обширных знаний об операциях и

процедурах телефонных компаний, что ему придется дозвониться до департамента Recent Change Memory Authorisation Center или RCMAC (Я всегда буду задавать себе вопрос – кто придумывает эти названия! Действительно необычно – это переводится как "Уполномоченный Центр Частой Смены Памяти " – прим. пер.). Он начал со звонка в коммерческий офис фирмы, сказал, что он из отдела ремонта и хотел узнать номер центра RCMAC, который обслуживал зону с названным им с кодом и префиксом, и он оказался тем же офисом, обслуживающим все линии тюрьмы. Эта была самая обычная услуга, предоставляемая техникам на работе, нуждающимся в помощи, и служащий незамедлительно дал номер.

Он позвонил в RCMAC, назвал «телефонное» имя и опять сказал, что он из отдела ремонта. Когда женщина ответила, Джонни спросил: «Установлен ли на номере deny terminate»?

«Да» – сказала она.

"Тогда это объясняет, почему клиент не может получать звонки… "– сказал Джонни. «Слушай, окажи мне, пожалуйста, услугу. Надо изменить свойство линии или убрать запрет входящих, ладно?» Возникла пауза, пока она проверяла другую компьютерную систему, есть ли приказ, разрешающий изменение. «Этот номер должен запрещать входящие звонки. Нет приказа об изменении».

«Тогда это ошибка... Мы должны были передать приказ вчера, но представитель счета заболела, и забыла попросить кого-либо отнести приказ за нее. Так что теперь клиентка бурно протестует по этому поводу».

После секундной паузы женщина обдумала просьбу, ведь просьба необычна и противоречит стандартным операциям, и сказала «Ладно». Он слышал, как она печатает, внося изменения. И через несколько секунд, все было сделано.

Лед тронулся, между ними образовалось нечто, похожее на сговор. Поняв отношение женщины и ее желание помочь, Джонни, не колеблясь, решил попробовать все сразу. Он сказал: «У тебя есть еще пару минут, чтобы помочь мне?»

«Да, – она ответила, – Что вам надо?»

«У меня есть еще пару линий, принадлежащих той же клиентке, и на всех та же проблема. Я прочту вам номера, чтобы вы проверили, поставлен ли на них запрет входящих – хорошо?» Она согласилась.

Через несколько минут, все линии были «починены» на прием входящих звонков.

Поиск Гондорффа

Теперь ему надо было узнать, в каком отделении находится Гондорфф. Это информация, которую люди, содержащие места заключения и тюрьмы, точно не захотят предоставить посторонним. Снова Джонни дол-

жен был положиться на свои навыки в социальной инженерии.

Он решил позвонить в тюрьму другого города – Майами, но любой другой бы подошел, и сказал, что он звонит из Нью-йоркской тюрьмы. Он попросил кого-нибудь, кто работает с компьютером центрального бюро, содержащего информацию обо всех заключенных, содержащихся в тюрьмах по всей стране.

Когда человек подошел к телефону, Джонни заговорил на своем Бруклиновском акценте. «Привет, – он сказал, – Это Томас из FDC (Federal detention center), Нью-Йорк. Наше подключение с центральным бюро не работает, не могли бы вы посмотреть расположение преступника для меня, мне кажется, он может быть в вашем учреждении», – и он сказал имя Гондорффа и регистрационный номер.

«Нет, он не здесь,» – сказал парень через несколько секунд. «Он в исправительном центре в Сан-Диего».

Джонни притворился удивленным. «Сан-Диего! Его должны были переправить в Майами на судебном самолете на прошлой неделе! Мы говорил об одном человеке – какая у него дата рождения?»

«12/3/60» сказал мужчина, прочитав с экрана.

«Да, это тот парень. В каком отделении он находится?»

«Он в Северном-10», сказал мужчина, беззаботно ответив на вопрос, не смотря на то, что не было ува-

жительной причины, зачем эта информация понадобилась работнику в Нью-Йорке.

Сейчас у Джонни были телефоны, включенные на прием входящих, и знал, в каком отделении находится Гондорфф. Теперь надо узнать, какой номер подключен к отделению Северное-10.

Это – сложная часть. Джонни позвонил на один из номеров. Он знал, что звонок телефона будет выключен; никто не узнает, что он звонит. Так что он сидел и читал туристический справочник *Величайшие Города Европы Фодора (Fodor's Europe's Great Cities),* слушая постоянные гудки в телефоне, пока наконец-то кто-то не поднял трубку. Заключенный на другом конце линии, конечно, будет пытаться добраться до своего адвоката, назначенного судом. Джонни подготовил ответ. "Офис Общественных Защитников, " – он объявил.

Когда мужчина попросил своего адвоката, Джонни сказал: «Я посмотрю, свободен ли он. Вы из какого отделения?» Он записал ответ мужчины, щелкнул по hold, вернулся через полминуты и сказал: «Он сейчас в суде, вам придется перезвонить позднее».

Он потратил большую часть утра, но могло быть и хуже; его четвертая попытка оказалась Северной-10. Теперь Джонни знал номер, соединенный с ООЗ в отделении Гондорффа.

Синхронизируй свои часы

Теперь надо передать сообщение Гондорффу, когда

ему надо поднять трубку, подключенную к Офису Общественных Защитников. Это было проще, чем может показаться.

Джонни позвонил в тюрьму, используя «официально – звучащий» голос, представился как сотрудник, и попросил, чтобы его соединили с Северным-10. Звонок соединили. Когда надзиратель поднял там трубку, Джонни обманул его, используя внутреннюю аббревиатуру для Приема и Выпуска (Recieving and Discharge), отдела, который работает с новыми и отбывающими заключенными: «Это Томас из П&В,» сказал он. «Я должен поговорить с заключенным Гондорффом. У нас есть некоторые его вещи, и он должен сообщит нам адрес, куда нам их лучше отправить. Не могли бы вы его позвать к телефону?»

Джонни слышал, как охранник кричит через комнату. Через несколько нетерпеливых минут, он услышал знакомый голос на линии.

Джонни сказал ему: «не говори ничего, пока я не объясню тебе, что я задумал». Он рассказал все предисловие так, чтобы казалось, будто Джонни обсуждает, куда он хочет доставить вещи. Потом он сказал: «если ты сможешь добраться до телефона офиса общественных защитников сегодня днем – не отвечай. А если не сможешь, назови время, когда ты сможешь быть там». Гондорфф не ответил. Джонни продолжил: «Хорошо. Будь там в час. Я тебе позвоню. Подними

трубку. Если он начнет звонить в Офис Общественных Защитников, нажимай на сброс каждые 20 секунд. Не переставай пробовать, пока не услышишь меня на другом конце».

В час дня, когда Гондорфф поднял трубку, Джонни уже ждал его. У них была живая, приятная, неторопливая беседа, начавшая серию подобных звонков, чтобы спланировать аферу, которая принесет деньги на оплату легальных счетов – свободных от правительственной завесы.

Анализ обмана

Этот эпизод показывает основной пример того, как социальный инженер может сделать то, что кажется невозможным, обманывая нескольких людей, каждый из которых делает нечто, кажущееся непоследовательным. На самом деле, каждое действие дает маленький кусочек головоломки, пока афера не закончена.

Первая сотрудница телефонной компании думала, что отдает информацию из гособслуживания.

Следующая сотрудница телефонной компании знала, что она не должна изменять класс линии без соответствующего приказа, но все равно помогла дружелюбному мужчине. Это дало возможность звонить во все 10 отделений тюрьмы.

Для мужчины из исправительной колонии в Майами, просьба помочь другому федеральному учреждению, у

которого проблемы с компьютером, звучала абсолютно убедительной. И даже если у него не было другой причины узнать номер отделения, почему бы не ответить на вопрос?

А охранник в Северном-10, поверивший, что собеседник действительно из этого же заведения, звонит по официальному делу? Это была полностью приемлемая просьба, так что он позвал заключенного Гондорффа к телефону. Совсем не серьезное дело.

Серия хорошо спланированных рассказов, которые складываются в единую цепь.

Быстрое скачивание

Через 10 лет после завершения юридического института, Нэд Рэсин видел своих одноклассников, живущих в маленьких миленьких домах с лужайками перед домом, членов различных клубов, играющих в гольф 2 раза в неделю, по-прежнему работая с копеечными делами людей, которым никогда не хватало денег на оплату счетов. Зависть может стать коварным спутником. Однажды Нэду это надоело.

Его единственный хороший клиент владел маленькой, но очень успешной бухгалтерской фирмой, которая специализировалась на покупках и объединениях. Они работали с Нэдом недолго, но достаточно, чтобы он понял, что они участвовали в сделках, которые могли бы повлиять на биржевую цену одной или двух компаний. Копеечное дело, но в чем-то оно лучше – маленький скачок в цене может стать большой процентной прибылью от инвестиций. Если бы только он мог заглянуть в их файлы, и посмотреть, над чем они работают…

Он знал человека, который знал человека, который разбирался в не совсем типичных вещах. Мужчина услышал план, зажегся и согласился помочь. За меньшую сумму, чем он обычно просил, вместе с процен-

том от прибыли с валютной биржи, мужчина рассказал Нэду, что надо делать. Он так же дал полезное маленькое устройство – новинку в магазинах.

Несколько дней подряд Нэд наблюдал за стоянкой в маленьком бизнес парке, где у бухгалтерской компании были непрезентабельные офисы, похожие на витрину магазина. Большинство людей уходило в 5:30-6:00. В 7 здание было пустым. Уборщики приезжали примерно в 7:30. Идеально.

На следующий вечер, за несколько минут до восьми, Нэд припарковал свою машину на стоянке фирмы. Как он и ожидал, она была пуста, не считая грузовика уборочной компании. Нэд, одетый в костюм и галстук, держа в руке потертый чемодан, приложил ухо к двери и услышал работающий пылесос. Он постучал очень громко. Ответ не последовал, но он был терпелив. Он постучал снова. Мужчина из уборочной команды наконец-то появился. «Здравствуй», кричал Нэд через стеклянную дверь, показывая пропуск одного из сотрудников, который он нашел чуть раньше. «Я закрыл свои ключи в машине и мне надо добраться до стола».

Мужчина открыл дверь, опять закрыл ее за Нэдом, и пошел по коридору, включая свет, чтобы Нэд видел, куда идти. А почему бы и нет – ведь он по идее один из тех, кто помогает ему класть еду на стол. По крайней мере, у него были все причины так думать.

Нэд сел за компьютер одного из сотрудников и вклю-

чил его. Пока он включал его, он установил устройство, которое ему дали, на порт USB, достаточно маленькое, чтобы носить в связке ключей, и, тем не менее способное умещать до 120 мегабайт информации. Он подключился к сети, используя логин и пароль секретарши сотрудника, приклеенный на бумажке к дисплею. Менее чем за 5 минут, Нэд скачал все файлы с таблицами и документами с рабочего компьютера и сетевых папок партнера, и уже направлялся к дому.

Сообщение от Митника

Промышленные шпионы и компьютерные взломщики иногда физически проникают в цель. Они не используют лом, чтобы пройти, социальные инженеры используют искусство обмана, чтобы повлиять на человека с другой стороны двери, который откроет дверь для него.

Легкие деньги

Когда а впервые познакомился с компьютерами в старших классах школы, нам приходилось подключаться к одному центральному миникомпьютеру DEC PDP 11, расположенному в пригороде Лос-Анджелеса, который использовали все школы Л.А. Операционная система на компьютере называлась RSTS/E, и эта была первая операционная система, с которой я научился работать.

В то время, в 1981 году, DEC устраивали ежегодную конференцию для своих пользователей, и в этом году конференция пройдет в Л.А. В популярном журнале для пользователей этой операционной системы было объявление о новой разработке по безопасности, Lock-11. Этот продукт продвигали с хорошей рекламной кампанией, где говорилось нечто вроде: «Сейчас 3:30 утра, и Джонни с другого конца улицы нашел ваш номер дозвона, 555-0336, с 336й попытки. Он внутри, а вы в пролете. Покупайте Lock-11». Продукт, как говорилось в рекламе, был «хакероустойчивым». И его собирались показать на конференции.

Я жаждал посмотреть на разработку. Друг старшеклассник, Винни, являвшийся моим партнером по хакингу в течение нескольких лет, впоследствии ставший

государственным информатором против меня, разделял мой интерес к новому продукту DEC, и воодушевил меня на поход на конференцию с ним.

Деньги на линии

Мы пришли и обнаружили большой переполох в толпе около презентации Lock-11. Похоже, что разработчики ставили деньги на то, что никто не сможет взломать их продукт. Звучит как вызов, перед которым я не смог устоять.

Мы направились прямо к стенду Lock-11, и обнаружили, что руководят там разработчики проекта; я узнал их, и они узнали меня – даже в юности у меня уже была репутация фрикера и хакера из-за большого рассказа в *LA Times* о моем первом контакте с властями. В статье рассказывалось, как я благодаря одним диалогам вошел посреди ночи в здание Pacific Telephone (телефонная компания – прим. переводчика), и вышел с компьютерными руководствами, прямо перед носом у их охраны. (Похоже, что *Times* хотели напечатать сенсационный рассказ, и в своих целях напечатали мое имя; я был еще несовершеннолетним, и статья нарушала не только традиции, а возможно даже закон о сокрытии имен несовершеннолетних, обвиненных в правонарушении.)

Когда Винни и я подошли, это вызвало интерес у обеих сторон. С их стороны был интерес, потому что они узнали во мне хакера, о котором читали, и были

немного шокированы, увидав меня. Интерес с нашей стороны вызвало то, что у каждого из трех разработчиков, стоявших там, был чек на $100, торчавший из значка участника конференции. В сумме приз для любого, кто сможет взломать их систему, составлял $300 – и это показалось большой суммой денег для пары тинэйджеров. Мы с трудом могли дождаться того, чтобы начать.

Lock-11 был спроектирован по признанному принципу, полагавшемуся на два уровня безопасности. У пользователя должен был быть верный идентификационный номер и пароль, но и вдобавок этот идентификационный номер и пароль будут работать, только если они введены с уполномоченного терминала, подход называемый *terminal-based security (безопасность, основанная на терминалах)* . Чтобы победить систему, хакеру бы понадобилось не только знание идентификационного номера и пароля, но и пришлось бы ввести информацию с правильного компьютера. Метод был хорошо признанным, и изобретатели Lock-11 были убеждены, что он будет держать плохих парней подальше. Мы решили преподать им урок, и заработать триста баксов.

Знакомый парень, который считался гуру в RSTS/E, уже подошел к стенду раньше нас. Несколько лет назад, он был одним из тех парней, кто озадачил меня взломом внутреннего компьютера разработчиков

DEC, после чего его сообщники выдали меня. Теперь он стал уважаемым программистом. Мы узнали, что он пытался взломать программу безопасности Lock-11, незадолго до того, как мы пришли, но не смог. Этот инцидент дал разработчикам еще большую уверенность, что их продукт действительно безопасен.

Соревнование было непосредственным испытанием: ты взламываешь – ты получаешь деньги. Хороший публичный трюк … если кто-нибудь не опозорит их и заберет деньги. Они были так уверены в своей разработке, и были достаточно наглыми, что даже приклеили распечатку на стенд с номерами учетных записей и соответствующих паролей в системе. Но не только пользовательские учетные записи, но и все привилегированные.

Это было гораздо менее приятно, чем звучит. С таким видом настроек, я знал, что каждый терминал подключен к порту на самом компьютере. Это – не ракетная физика, чтобы догадаться, что они установили пять терминалов в зале для конференций, и посетитель мог войти только как непривилегированный пользователь – это значит, что подключения были возможны только с учетных записей с правами системного администратора. Похоже, что было только два пути: обойти систему безопасности, для предотвращения чего и был рассчитан Lock-11, или как-нибудь обойти программное обеспечение, как разработчики даже

не представляли.

LINGO

Terminal-based security – Безопасность, частично основанная на идентификации конкретного используемого компьютера; этот метод был особо популярен с главными компьютерами IBM.

Вызов принят

Мы с Винни уходили и говорили о конкурсе, и я придумал план. Мы невинно ходили вокруг, поглядывая на стенд с расстояния. Во время обеда, когда толпа разошлась, и трое разработчиков решили воспользоваться перерывом и пошли вместе купить себе что-нибудь поесть, оставив женщину, которая могла быть женой или девушкой одного из них. Мы прогуливались туда-сюда, и я отвлекал женщину, разговаривал с ней о разных вещах: «давно ли ты работаешь в компании?», «какие еще продукты вашей компании имеются в продаже» и т.д.

Тем временем, Винни, вне поля ее зрения, приступил к работе, используя навыки, которые мы развивали. Помимо очарованности взломом компьютеров и моего интереса к магии, мы были заинтересованы в обучении открытия замков. Когда я был маленьким, я прочесывал полки подпольного книжного магазина в Сан-Франциско, в котором были тома о вскрытии замков, вылезании из наручников, создании поддельных удостоверений – и о других вещах, о которых дети не

должны знать.

Винни, как и я, тренировался вскрывать замки до тех пор, пока у нас не стало хорошо получаться с замками магазинов с железом. Было время, когда я устраивал розыгрыши – находил кого-нибудь, кто использовал 2 замка для безопасности, вскрывал их и менял местами, и это очень удивляло и расстраивало, если он пытался открыть их не тем ключом.

В выставочном зале, я продолжал отвлекать девушку, пока Винни подполз сзади будки, вскрыл замок в кабинет, где стоял их PDP-11 и кабели. Назвать кабинет запертым – это почти шутка. Он был защищен тем, что слесари называют wafer lock(вафельный замок), известный как легко открываемый, даже для таких неуклюжих любителей взламывать замки как мы.

Винни понадобилась примерно минута, чтобы открыть замок. Внутри, в кабинете он обнаружил то, что мы не любили: полосы портов, для подключения пользовательских терминалов, и один порт, который называется консольным терминалом. Этот терминал использовался оператором или системным администратором, чтобы управлять всеми компьютерами. Винни подключил кабель, идущий от консольного порта к одному из терминалов, находящихся на выставке.

Это означало, что теперь этот терминал воспринимается как консольный терминал. Я сел за переподключенную машину, и использовал пароль, кото-

рый так смело предоставили разработчики. Поскольку Lock-11 определил, что я подключаюсь с уполномоченного терминала, он дал мне доступ, и я был подключен с правами системного администратора. Я пропатчил операционную систему, изменил ее так, что можно будет подключиться с любого компьютера на этаже в качестве привилегированного пользователя.

Когда я установил свой секретный патч, Винни вернулся к работе, отключил терминальный кабель и подключил его туда, где он был первоначально. Он еще раз вскрыл замок, на этот раз, чтобы закрыть дверь кабинета.

Я сделал листинг директорий, в поисках папок и программ, связанных с Lock-11, и случайно наткнулся на кое-что шокирующее: директория, которая не должна была быть на этой машине. Разработчики были слишком уверены, что их программное обеспечение непобедимо, что они даже не побеспокоились о том, чтобы убрать исходный код их нового продукта. Я передвинулся к соседнему печатающему терминалу, и начал распечатывать порции исходного кода на длинных листах зелено-полосатой бумаги, используемой компьютерами в те времена.

Винни едва успел закрыть замок и вернуться ко мне, когда парни вернулись с обеда. Они застали меня, сидящего возле компьютера бьющего по клавишам, а принтер продолжал печатать. «Что делаешь, Кевин?»–

спросил один из них.

"А, просто печатаю исходники, “ я сказал. Они предположили, что я шучу. Пока не посмотрели на принтер и не увидели, что это *действительно* тот ревностно охраняемый исходный код их продукта.

Они не поверили, что я действительно подключился как привилегированный пользователь. «Нажми Control-T,» – приказал один из разработчиков. Я нажал. Надпись на экране подтвердила мое утверждение. Парень ударил рукой по своему лбу, когда Винни говорил «Триста долларов, пожалуйста».

Сообщение от Митника

Вот еще один пример того, как умные люди недооценивают противника. А как насчет вас – вы уверены, что можно поставить $300 на ваши охранные системы, против взломщика? Иногда обход вокруг технологических устройств не такой, какой вы ожидаете.

Они заплатили. Мы с Винни ходили по выставке оставшуюся часть дня со стодолларовыми чеками, прикрепленными к нашим значкам конференции. Каждый, что видел чеки, знал, что они означают.

Конечно, мы с Винни не победили их программу, и если разработчики установили бы хорошие правила в конкурсе или использовали бы действительно безопасный замок, или присматривали за своим оборудованием более внимательно, то им бы не пришлось терпеть унижение того дня – унижение из-за парочки под-

ростков.

Позже, я узнал, что команде разработчиков пришлось зайти в банк, чтобы получить наличные: эти стодолларовые чеки – все деньги, взятые с собой, которые они собирались тратить.

Словарь как орудие атаки

Когда кто-нибудь получает ваш пароль, он может вторгнутся в вашу систему. В большинстве случаев, вы даже не узнаете, что произошло что-то плохое.

У юного хакера, которого я назову Иваном Питерсом, есть цель – получить исходный код для новой электронной игры. У него не было проблем с проникновением в сеть компании, потому что его друг-хакер уже скомпрометировал один из веб-серверов фирмы. Найдя непропатченную уязвимость в программном обеспечении веб-сервера, его друг чуть не свалился со стула, узнав что система была настроена в как *dual-homed host* , что означало, что у него был входной пункт в локальную сеть фирмы.

Но когда Иван подключился, он столкнулся с испытанием, похожим на хождение по Лувру в надежде найти Мона Лизу. Без карты, вы можете бродить неделями. Компания была международной, с сотнями офисов и тысячами компьютерных серверов, и они не предоставили список систем разработчиков или услуги туристического гида, чтобы сразу привести его к нужному.

Вместо того, чтобы использовать технический подход, чтобы узнать, какой сервер является его целью, он использовал социально-инженерный подход. Он зво-

нил, основываясь на методах, похожих на описанные в этой книге. Сначала, позвонил в службу технической поддержки, и заявил, что он сотрудник компании, у которого проблемы с интерфейсом в продукте, который разрабатывала его группа, и спросил телефон руководителя проекта группы разработчиков игры.

Потом он позвонил тому, чье имя ему дали, и представился как тот парень из техподдержки. «Позже ночью», сказал он, «мы будем заменять роутер и должны убедиться, что люди из твоей группы не потеряют связь с сервером. Поэтому мы должны знать, какие серверы использует ваша команда.» В сети постоянно производился апгрейд. И сказать название сервера никому и никак не повредит, верно? Раз он был защищен паролем, всего лишь сказав имя, это не помогло бы никому взломать его. И парень сказал атакующему имя сервера. Он даже не позаботился о том, чтобы перезвонить парню и подтвердить рассказ, или записать его имя и телефон. Он просто сказал имена серверов, ATM5 и ATM6.

Атака паролями

В этом месте Иван использовал технический подход для получения удостоверяющей информации. Первый шаг в большинстве технических взломов систем, предоставляющих удаленный доступ – найти аккаунт со слабым паролем, который даст первоначальный доступ к системе.

Когда атакующий пытается использовать хакерские инструменты для паролей, работающих удаленно, может понадобится оставаться подключенным к сети компании в течение нескольких часов за раз. Он делает это на свой риск: чем дольше он подключен, тем больше риск, что его обнаружат и поймают.

В качестве начального этапа Иван решил сделать подбор пароля, который покажет подробности о системе (возможно, имеется ввиду, что программа показывает логины – прим. пер.). Опять-таки, интернет удобно преоставляет ПО для этой цели (на **http://ntsleuth.0catch.com** ; символ перед «catch» – ноль). Иван нашел несколько общедоступных хакерских программ в сети, автоматизирующих процесс подбора, избегая необходимости делать это вручную что займет больше времени, и следовательно работает с большим риском. Зная, что организация в основном работала на основе серверов Windows, он сказал копию NBTEnum, утилиту для подбора пароля к NetBIOS(базовая система ввода/вывода). Он ввел IP (Internet Protocol) адрес сервера ATM5, и запустил программу.

LINGO

Enumeration – Процесс, показывающий сервисы, работающие на системе, операционную систему и список имен аккаунтов пользователей, у которых есть доступ к стстеме.

Программа для подбора смогла определить не-

сколько учетных записей, существовавших на сервере. Когда существующие аккаунты были определены, та же программа подбора получила возможность начать атаку по словарю против компьютерной системы. Атака по словарю – это что-то, что знакомо парням из службы компьютерной безопасности и взломщикам, но многие будут поражены, узнав что это возможно. Такая атака нацелена на раскрытие пароля каждого пользователя, используя частоупотребляемые слова.

Мы все иногда ленимся в некоторых вещах, но меня никогда не перестает удивлять, что когда люди выбирают пароли, их творческий подход и воображение, похоже, исчезают. Многие из нас хотят пароль, который одновременно даст защиту и его легко запомнить, что означает, что это что-то близкое для нас. К примеру, наши инициалы, второе имя, ник, имя супруга, любимая песня, фильм или напиток. Название улицы, на которой мы живем, или города, где мы живем, марка машины, на которой мы ездим, деревни у берега на Гавайях, где мы любим отдыхать, или любимый ручей, где лучше всего клюет форель. Узнаете структуру? В основном, это все – имена собственные,названия мест или слова из словаря. Атака словарем перебирает частоиспользуемые слова с очень быстрой скоростью, проверяя каждый пароль на одном или более пользовательских аккаунтов.

Иван устроил атаку в трех частях. В первой он ис-

пользовал простой список из 800 самых обычных паролей; список включает *secret*, *work* и *password* . Программа также изменяла слова из списка, и пробовала каждое с прибавленным числом, или прибавляла численное значение текущего месяца. Программа попробовала каждый раз на всех найденных пользовательских аккаунтах. Никакого везения.

Для следующей попытки, Иван пошел на поисковую систему Google, и ввел «wordlist dictionaries,» и нашел тысячи сайтов с большими списками слов и словарями на английском и на некоторых иностранных языках. Он скачал целый электронный английский словарь. Он улучшил его, скачав несколько словарей, найденных в Google. Иван выбрал сайт **www.outpost9.com/files/WordLists.html** .

На этом сайте он скачал (и все это – *бесплатно*) подборку файлов, включая фамилии, вторые имена, имена и слова членов конгресса, имена актеров, и слова и имена из Библии.

Еще один из многих сайтов, предлагающих списки слов предоставляется через Оксфордский университет, на **ftp://ftp.ox.ac.uk/pub/wordlists** .

Другие сайты предоставляют списки с именами героев мультфильмов, слов, использованных у Шекспира, в Одиссее, у Толкина, в сериале Star Trek, а также в науке и религии и так далее (одна онлайновая компания продает список, состоящий из 4,4 миллионов слов

и имен всего за $20). Атакующая программа также может быть настроена на проверку анаграмм слов из словаря – еще один любимый метод, который, по мнению пользователей компьютера, увеличивает их безопасность.

Быстрее, чем ты думаешь

Когда Иван решил, какой список слов использовать, и начал атаку, программное обеспечение заработало на автопилоте. Он смог обратить свое внимание на другие вещи. А вот и удивительная часть: вы думаете, что такая атака позволит хакеру поспать, и программа все равно сделала бы мало, когда он проснется. На самом деле, в зависимости от атакуемой операционной системы, конфигурации систем безопасности и сетевого соединения, каждое слово в Английском словаре может быть перепробовано менее, чем за 30 минут!

Пока работала эта атака, Иван запустил похожую атаку на другом компьютере, нацеленную на другой сервер, используемый группой разработчиков, ATM6. Через 20 минут, атакующая программа сделала то, что многие неподозревающие пользователи считают невозможным: она взломала пароль, показывая, что один из пользователей выбрал пароль «Frodo», один из хоббитов из книги *Властелин Колец* .

С паролем в руке, Иван смог подключиться к серверу ATM6, используя пользовательский аккаунт.

Для нашего атакующего была хорошая и плохая но-

вости. Хорошая новость – у взломанного аккаунта были администраторские права, которые были нужны для следующего этапа. А плохая новость – то, что исходный код игры нигде не был обнаружен. Он должен быть, все-таки, на другом компьютере, ATM5, который, как он уже узнал, смог устоять перед атакой по словарю. Но Иван еще не сдался; он еще должен был попробовать несколько штучек.

На некоторый операционных системах Windows и Unix, хэши (зашифрованные пароли) с паролями открыто доступны любому, кто получает доступ к компьютеру, на котором они находятся. Причина в том, что зашифрованные пароли не могут быть взломанными, а следовательно, и не нуждаются в защите. Эта теория ошибочна. Используя другую программу, pwdump3, также доступную в Интернете, он смог извлечь хэши паролей с компьютера ATM6 и скачать их.

Типичный файл с хэшами паролей выглядит так:

```
Administrator:500:95E4321A38AD8D6AB75E0C8D769
akasper:1110:5A8D7E9E3C3954F642C5C736306CBF
digger:1111:5D15C0D58DD216C525AD3B83FA6627C
elligan:1112:2017D4A5D8D1383EFF17365FAF1FFE89
tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404E
vkantar:1116:81A6A5D035596E7DAAD3B435B51404E
vwallwick:1119:25904EC665BA30F449AF4449AF42E1
mmcdonald:1121:A4AED098D29A3217AAD3B435B51
kworkman:1141:C5C598AF45768635AAD3B435B5140
```

С хэшами, скачанными на его компьютер, Иван использовал другую программу, делавшую другой вид атаки, известную как brute force(брутфорс). Этот тип атаки пробует каждую комбинацию цифровых, буквенных и специальных символов.

Иван использовал утилиту под названием L0phtcrack3 (произносится лофт-крэк; доступно на **www.atstake.com** ; еще один ресурс для отличных программ, вскрывающих пароли – **www.elcomsoft.com**). Системные администраторы используют L0phtcrack3 для проверки «слабых» паролей; атакующие используют его для взлома паролей. Функция брутфорса в LC3 пробует пароли с комбинациями букв, цифр, и большинства символов, включая **!@#$%** ^&. Она систематически перебирает каждую возможную комбинацию из большинства символов (Запомните, однако, что если используются непечатаемые символы, LC3 не сможет открыть пароль).

У программы почти невероятная скорость, которая может достигать 2.8 миллионов попыток в секунду на компьютере с процессором с частотой 1ГГц. Но даже с такой скоростью, если системный администратор правильно настроил операционную систему Windows (отключив использование хэшей LANMAN),взлом пароля может занять много времени.

LINGO

Атака брутфорсом Стратегия обнаружения паро-

ля, которая пробует каждую возможную комбинацию буквенных, численных и специальных символов.

По этой причине атакующий часто скачивает хэши и запускает атаку на своем или чужом компьютере, а не остается подключенным к локальной сети компании, рискуя быть обнаруженным.

Для Ивана ожидание не было долгим. Через несколько часов, программа предоставила ему пароли каждого члена из команды разработчиков. Но это были пароли пользователей сервера ATM6, и он уже знал, что исходный код, который он искал, был не на этом сервере.

Что же дальше? Он все равно не смог получить пароль для аккаунта на компьютере ATM5. Используя свой хакерский стиль мышления и понимая неправильные небезопасные привычки пользователей, он предположил, что один член команды (разработчиков) мог выбрать одинаковые пароли на обеих компьютерах.

На самом деле, именно это он и обнаружил. Один из членов команды использовал пароль «gamers» на ATM5 и ATM6.

Дверь широко открылась перед Иваном, и он нашел программы, которые он искал. Когда он обнаружил исходники и радостно скачал их, и сделал еще один шаг, типичный для взломщиков систем: он сменил пароль неиспользуемого аккаунта с администраторскими правами, в случае если он захочет получить более новую

версию программного обеспечения в будущем.

Анализ обмана

В этой атаке, основывавшейся на технических и человеческих уязвимостях, атакующий начал с предварительного звонка, чтобы узнать местоположение и имена серверов разработчиков, на которых была частная информация.

Он использовал программу, чтобы узнать имена пользователей аккаунтов каждого, у кого был аккаунт на сервере разработчиков. Потом он провел две успешных атаки на пароли, включая атаку по словарю, которая ищет частоиспользуемые пароли, перебирая все слова в английском словаре иногда дополненный несколькими списками слов, содержащих имена, места и специализированные предметы.

Так как коммерчесие и общественные программы для взлома могут быть получены каждым для любых целей, важно, чтобы вы были бдительны при защите компьютерных систем предприятия и сетевой инфраструктуры.

Важность этой угрозы не может быть переоценена. По данным журнала *Computer World*, исследования в Oppenhiemer Funds в Нью-Йорке привели к поразительному открытию. Вице-президент фирмы по сетевой безопасности произвел атаку на пароли, используемые сотруднами фирмы, применявших один из стандартных пакетов ПО. Журнал сообщает, что за *три ми-*

нуты он смог узнать пароли 800 сотрудников.

Сообщение от Митника

Если воспользоваться терминологией игры «Монополия», если вы используете словарное слово в качестве пароля – отправляйтесь сразу в тюрьму. Не проходите поле «Вперед», вы не получите $200.(Максимально приближено к русской версии монополии, хотя точно не помню)

Предотвращение обмана

Атаки социальных инженеров могут стать еще более деструктивными, когда атакующий использует элементы технологии. Предотвращение этого вида атаки обычно включает в себя меры безопасности на человеческом и технологическом уровне.

Просто скажи «Нет»

В первой истории в этой главе, служащий компании RCMAC не должен был снимать статус deny terminate с 10 телефонных линий без ордера, подтверждающего изменение. Недостаточно того, чтобы сотрудники знали правила безопасности и процедуры; сотрудники должны понимать, насколько важны эти правила для компании для предотвращения нанесения ущерба.

Правила безопасности должны не должны поощрять отклонение от процедуры, используя систему поощрений и последствий. Естественно, правила безопасности должны быть реалистичными, не призывающие сотрудников выполнять слишком обременительные вещи, которые, скорее всего, будут проигнорированы. Также, программа обучения (ликбеза) по безопасности должна убедить служащих, что надо выполнять поручения по работе быстро, но кратчайший путь, пренебрегающий системой безопасности, может оказаться

вредным для компании и сотрудников.

Та же осторожность должна присутствовать при предоставлении информации незнакомому человеку по телефону. Не смотря на то, как убедительно он представил себя, невзирая на статус или должность человека в компании, *никакая* информация, которая не предназначена для общественного доступа, не должна быть предоставлена, пока личность звонящего не будет установлена. Если бы эти правила строго соблюдались, социально-инженерный план в этом рассказе потерпел бы неудачу, и федеральный заключенный Гондорфф никогда не смог бы спланировать еще одну аферу с его приятелем Джонни.

Этот единственный пункт настолько важен, что я повторяю его на протяжении всей книги: проверяйте, проверяйте, проверяйте. Каждая просьба, не сделанная лично, никогда не должна быть выполнена без подтверждения личности просящего – и точка.

Уборка

Для любой фирмы, у которой нет охранников круглосуточно, план, где атакующий получает доступ к офису на несколько часов – трудность. Уборщики обычно относятся с с уважением к каждому, кто кажется членом компании и не выглядит подозрительно. Все-таки, этот человек может вызвать у них неприятности или уволить. По этой причине уборщики, как сотрудники фирмы так и работающие по контракту из внешнего агент-

ства, должны быть обучены технике безопасности.

Уборочная работа не требует образования в колледже и даже умения говорить по-английски, и даже если требует обучения, то не по безопасности, а только по использованию разных очистительных средств для разных назначений. Обычно эти люди даже не получают указаний вроде: «если кто-нибудь попросит вас впустить их после рабочего времени, вы должны проверить у них пропуск, позвонить в офис уборочной компании, объяснить ситуацию и подождать разрешения».

Организации нужно заранее спланировать, что делать в конкретной ситуации, как эта, прежде чем она произойдет и соответственно обучить людей. По моему опыту, я узнал что большинство, если не весь частный бизнес неточен в этой части физической безопасности. Вы можете попробовать подойти к проблеме с другой стороны, возложив бремя на сотрудников своей компании. Компании без круглосуточной охраны должны сообщать сотрудникам, что если им понадобится войти после рабочего дня, им придется воспользоваться собственными ключами или электронными картами, и не должны ставить уборщиков в положение выбора, кого можно пропустить. Сообщите уборочной компании, что их люди должны быть обучены не впускать кого-либо в помещение в любое время. Это простое правило – никому не открывайте дверь. Если нужно, то это может быть включено в контракт с уборочной ком-

панией.

Также уборщики должны знать о технике «piggyback»(посторонние люди следуют за уполномоченным человеком через безопасный вход). Они должны быть обучены не разрешать другим людям входить в здание только потому, что он выглядит как сотрудник.

Примерно три или четыре раза в год устраивайте тест на проникновение или оценку уязвимости. Попросите кого-нибудь подойти к двери, когда работают уборщики, и попробуйте проникнуть в здание. Но лучше не используйте для этого собственных сотрудников, а наймите сотрудников фирмы, специализирующейся на этом виде тестов на проникновение.

Передай другому: Защити свои пароли

Организации становятся все более и более бдительными, усиливая технику безопасности техническими методами, например, конфигурируя операционную систему усложнять технику безопасности паролей и ограничить число неверных вводов перед блокированием аккаунта. На самом деле, такое свойство встроено в платформы Microsoft Windows, которые предназначены для бизнеса. Но, зная как раздражают покупателей свойства, которые требуют лишних усилий, продукты обычно поставляются с отключенными функциями. Уже пора бы разработчикам прекратить поставлять продукты с отключенными по умолчанию функциями безопасности, когда все должно быть наоборот(я по-

дозреваю, что в скором времени они догадаются).

Конечно, правила безопасности корпорации должны разрешать системным администраторам дополнять эти правила техническими методами, когда возможно, с учетом того, что людям свойственно ошибаться. Понятно, что если вы, к примеру, ограничите число неверных попыток входа через конкретный аккаунт, то вы сможете сделать жизнь атакующего более тяжелой.

Каждая организация сталкивается с нелегким выбором между мощной безопасностью и продуктивностью сотрудников, что заставляет некоторых сотрудников пренебрегать правилами безопасности, не понимая, насколько они необходимы для защиты целостности секретной компьютерной информации.

Если правила безопасности не будут конкретно указывать возможные проблемы при пренебрежении ими, сотрудники могут пойти по пути наименьшего сопротивления, и сделать что-либо, что облегчит их работу. Некоторые сотрудники могут открыто пренебрегать безопасными привычками. Вы могли встречать сотрудников, кто следует правилам о длине и сложности пароля, но записывает пароль на листок бумаги и клеит его к монитору.

Жизненно-важная часть защиты организации – использование сложно угадываемых паролей в сочетании с мощными настройками безопасности в технике.

Подробное обсуждене рекомендованной техники

безопасности паролей описано в главе 16.

Глава 13: Умные мошенники

Перевод: matt weird (mattweird@whoever.com)

Теперь вы выяснили, что когда незнакомец звонит с запросом на чувствительную информацию или на что-то, что может представлять ценность для атакующего, человек, принимающий звонок, должен быть обучен требовать телефонный номер вызывающего и перезванивать чтобы проверить, что человек на самом деле есть тот, за кого себя выдает – сотрудник компании, или сотрудник партнера по бизнесу, или представитель службы технической поддержки от одного из ваших поставщиков, например.

Даже когда компания установила процедуру, которой сотрудники тщательно следуют для проверки звонящих, сообразительные атакующие все еще способны использовать набор трюков для обмана своих жертв, заставляя поверить что они те, за кого себя выдают. Даже сознательные в отношении безопасности сотрудники могут стать обманутыми методами, такими как нижеприведенные.

Несоответствующий “Caller ID”

Любой кто хоть раз получал звонок на сотовой телефон, наблюдал в действии опцию, называемую “caller ID”(дословно “Идентификатор Вызывающего”) – этот знакомый дисплей, отображающий телефонный номер звонящего. В рабочей обстановке эта функция предлагает возможность рабочему одним взглядом оценить, от знакомого ли сотрудника идет вызов или же откуда-то вне компании.

Много лет назад некие амбициозные телефонные фрикеры обнаружили для себя все прелести caller ID еще даже до того как телефонная компания публично стала предлагать подобный сервис абонентам. Они изрядно повесилились, одурачивая людей ответами по телефону и приветствуя вызывающего по имени, в то время как тот даже не успевал сказать ни слова.

Просто когда вы думаете что подобное безопасно, практика удостоверения личности путем доверия тому что вы видите – то, что появляется на дисплее caller ID – это именно то, на что атакующий может расчитывать.

Звонок Линды

День/время: Вторник, 23 июля, 15:12

Место: “Офисы Финансового Отдела, Авиакомпания Starbeat”

Телефон Линды Хилл зазвонил когда она записывала заметку для босса. Она взглянула на дисплей caller ID, который показывал что звонок исходил из офиса корпорации в Нью Йорке, но от кого-то по имени Виктор Мартин – имя она не узнала.

Она подумала дождаться пока звонок переключится на автоответчик, так что ей не придется отрываться от мысли заметки. Но любопытство взяло верх. Она подняла трубку и звонящий представился и сказал что он из отдела рекламы и работает над некоторым материалом для управляющего компании. “Он на пути к деловой встрече в Бостоне с кем-то из банкиров. Ему требуется первоклассный финансовый отчет на текущий квартал,” сказал он. “И еще одна вещь. Еще ему нужны финансовые прогнозы на проект Апачи,” добавил Виктор, используя кодовое название продукта, который был одним из главных релизов этой весной.

Она попросила его электронный адрес, но он сказал что у него проблема с получением электронной почты и над этим работает служба технической поддержки, поэтому не могла бы она использовать факс взамен? Она сказала что это тоже подойдет, и он дал дополнительный внутренний код для его факс-машины.

Она отослала факс несолькими минутами позже.

Но Виктор не работал в отделе рекламы. К слову сказать, он даже в компании-то не работал.

История Джека

Джек Доукинс начал свою “профессиональную” карьеру в раннем возрасте в качестве карманного вора, промышляя на спортивных играх на стадионе команды Янки в оживленных помещениях под трибунами и среди ночной толпы туристов на Таймс-Скуэйр. Он так проворно и искусно доказывал что мог снять часы с запястья человека, так что тот даже не узнает. Но в его трудные подростковые годы он рос неуклюжим и не был неуловим. В компании Джувенил Холл(дворец молодежи?)) Джек обучился новому ремеслу с куда меньшим риском быть схваченным.

Его текущее назначение взывало его получать информацию о квартальном доходе, издержках и финансовом потоке компании до того как эти данные подавались в Комиссию по Обмену и Ценным Бумагам и обнародовались. Его клиентом был дантист, который не хотел объяснять почему он хотел получить информацию. Предусмотрительность этого человека показалась Джеку смехотворной. Подобное он видел и до этого – у парня наверное была проблема с азартными играми, или может недешево обходящаяся любовница, о которой его жена была еще не в курсе. Или может быть он просто хвастался своей жене насчет того, как он умен на фондовой бирже; теперь же он петерял пару пакетов акций и хотел сделать нехилое вложение в нечто более надежное, зная как именно биржевая стоимость компании будет прогрессировать ко-

гда они анонсируют квартальные итоги.

Люди удивляются когда обнаруживают как мало времени требуется социальному инженеру чтобы выяснить как контролировать ситуацию, с которой он прежде никогда не сталкивался. К тому времени как Джек вернулся домой с его встречи с дантистом, у него уже сформировался план. Его друг Чарлз Бэйтс работал в компании Панда Импорт, у которой был свой собственный телефонный коммутатор, или PBX.

В терминах, близких людям, знающим телефонные системы, PBX был подключен к цифровой телефонной службе известной как T1, сконфигурированной как Интерфейс Основного Тарифного плана цифровой сети интегрированных услуг (Primary Rate Interface ISDN(integrated services digital network), PRI ISDN – выделенный канал). Под этим подразумевается, что каждый раз когда звонок исходил от Панда Импорт, установки и другая информация обработки вызова попадали из канала данных в телефонный коммутатор компании; информация включала в себя номер вызывающей стороны, который(если не заблокирован) передавался в устройство caller ID на конце линии получателя.

Друг Джека знал как запрограммировать коммутатор так, чтобы человек, получающий вызов, видел бы на его caller ID-дисплее не действительный телефонный номер в офисе Панда Импорт, а какой угодно другой номер, который он запрограммировал в коммутатор.

Этот трюк работает, поскольку местные телефонные компании не беспокоятся о подтверждении номера вызывающего, полученного от абонента, и сравнении его с действительными телефонными номерами за которые абонент платит.

Все что Джеку Доукинсу было нужно – это доступ к любому такому телефонному сервису. К счастью, его друг и временами партнер по преступлениям, Чарльз Бэйтс, всегда был рад протянуть руку помощи за соответствующее вознагрждение. В данном случае, Джек и Чарльз временно перепрограммировали телефонный коммутатор так, что звонки с конкретной телефонной линии, проходящей в зданиях Панда Импорт, подменяли бы внутренний телефонный номер Виктора Мартина, делая похожим что вызов идет из авиакомпании Starbeat.

Идея того, что ваш caller ID может быть изменен для отображения любого желаемого вами номера, так малоизвестна, что редко ставится под вопрос. В данном случае, Линда была счастлива отправить факсом запрошенную информацию парню, который, как она думала, был из рекламного отдела.

Когда Джек повесил трубку, Чарльз перепрограммировал телефонный коммутатор компании, вернув телефонный номер к исходным установкам.

Анализ обмана

Некоторые компании не хотят чтобы их клиенты или

поставщики знали телефонные номера их сотрудников. Например, в компании Ford могут решить, что звонки из их Центра Службы Поддержки Потребителей должны отображать номер 800 для Центра и имя вроде “Поддержка Ford” вместо реального прямого телефонного номера каждого представителя слубы поддержки, осуществляющего звонок. Microsoft может захотеть дать своим сотрудникам возможность говорить людям свой телефонный номер вместо того, чтобы каждый, кому они звонят, кидал взгляд на их caller ID и знал их дополнительный код. Таким способом компания способна поддерживать конфиденциальность внутренних номеров.

Но эта же самая возможность перепрограммирования предоставляет удобную тактику для хулигана, коллекционера счетов, телемаркетолога, и, конечно же, социального инженера.

Вариация: Звонит президент Соединенных Штатов

Как соведущий радиошоу в Лос Анджелесе, которое называется “Темная сторона Интернета” на KFI Talk Radio, я работал под руководством директора по программам станции. Дэвида, одного из самых посвященных и вкалывающих людей которых я когда-либо встречал, очень сложно застать по телефону, так как он очень занят. Он один из тех людей, который не отвечает на звонок, если только не видит на caller ID-дисплее что это кто-то с кем ему нужно поговорить.

Когда я ему звонил, по причине наличия блокировки вызова на моем сотовом телефоне, он не мог сказать кто звонил и не отвечал на звонок. Звонок переключался на автоответчик, и для меня это стало изматывающим.

Я переговорил по поводу того, что с этим делать с моим давним другом, основателем фирмы по работе с недвижимостью, предоставлявшей офисные помещения для хайтек-компаний. Вместе мы разработали план. У него был доступ к телефонному коммутатору Meridian его компании, который дает ему возможность программирования номера вызывающей стороны, как описано в предыдущей истории. В любой мо-

мент, когда мне было нужно дозвониться до директора по программам и не удавалось пробиться, я просил своего друга запрограммировать любой номер на мой выбор, который должен был появится на caller ID. Иногда он делал так, чтобы выглядело что звонок исходит от офисного ассистента Дэвида, или иногда от холдинговой компании, которая владеет станцией.

Но самым излюбленным было запрограммировать звонок, как будто он с собственного домашнего телефонного номера Дэвида, на который он всегда снимал трубку. Черт возьми, однако надо отдать этому парню должное. У него всегда было хорошее чувство юмора на этот счет, когда он брал трубку и обнаруживал что я его снова одурачил. Самым лучшим было то, что он оставался на линии достаточно долго чтобы выяснить чего я хотел и разрешить любую неувязку, какой бы она не была.

Когда я демонстрировал этот маленький трюк на шоу Арта Белла, я подменил свой caller ID так, чтобы он отображал имя и адрес штабквартиры ФБР в Лос Анджелесе. Арт был совершенно шокирован по поводу всей затеи и убеждал меня в совершении чего-то нелегального. Но я указал ему на то, что это вполне легально, до тех пор пока это не является попыткой совершения мошенничества. После программы я получил несколько сотен писем по электронной почте с просьбой объяснить как я это сделал. Теперь вы знаете.

Это совершенный инструмент для построения убедительности социального инженера. Если, для примера, в течение исследовательской стадии цикла атаки социального инжиниринга было обнаружено, что у цели был caller ID, атакующий мог бы подменить его или ее собственный номер как будто будучи от доверительной компании или сотрудника. Коллекционер счетов может выдать его или ее звонки за исходящие с вашего места работы.

Но остановитесь и задумайтесь о подтекстах. Компьютерный злоумышленник может позвонить вам на дом, утверждая что он из отдела Информационных Технологий в вашей компании. Человеку на линии насущно требуется ваш пароль для восстановления ваших файлов после сбоя сервера. Или caller ID показывает имя и номер вашего банка или брокерского дома, девушке с милым голосом просто понадобилось проверить номер вашего счета и девичью фамилию вашей матери. Для ровного счета, ей так же нужно проверить ваш ATM PIN[2] по причине какой-то системной проблемы. Управление котельной на фондовой бирже может сделать свои звонки похожими на исходящие от Мэрил Линч или Городского Банка. Кто-то вознамерился украсть вашу личность и позвонить, очевидно из ком-

---

[2] Automated Teller System Personal Identifiacation Number – персональный идентификационный номер для системы “автоматизированный кассир”

пании Visa, и убедить вас сказать ему номер вашей кредитной карты Visa. Злостный парень мог бы позвонить и заявить, что он из налоговой инспекции или ФБР.

Если у вас есть доступ к телефонной системе, подключенной к Интерфейсу Основного Тарифа(PRI), плюс небольшие познания в программировании, которые вы, вероятнее всего, приобретете на веб-сайте поставщика системы, вы сможете использовать такую тактику для разыгрывания крутых трюков над своими друзьями. Есть на примете кто-нибудь с раздутыми политическими устремлениями? Вы бы могли запрограммировать выдаваемый номер как 202 456-1414, и его caller ID-дисплей будет показывать имя “БЕЛЫЙ ДОМ.”

Он подумает что ему звонит президент!

Мораль истории проста: нельзя доверять caller ID, за исключением использования для проверки внутренних звонков. На работе или дома, все должны остерегаться трюка с caller ID и иметь ввиду что имени или телефонному номеру, отображаемому на caller ID-дисплее, нельзя доверять для удостоверения личности.

Сообщение от Митника

В следующий раз, когда вам звонят и ваш caller ID-дисплей показывает что звонок от вашей дорогой престарелой мамы, никогда не знаешь – он может быть от старого доброго социального инженера.

Невидимый сотрудник

Ширли Кутласс нашла новый и захватывающий путь сделать быстрые деньги. Больше не надо долгими часами вкалывать на соляной шахте. Она присоединилась к сотням других артистов-мошеннков, вовлеченных в преступление десятилетия. Она вор личности.

Сегодня она устремила свои взгляды на получение конфиденциальной информации от службы поддержки потребителей компании, занимающейся кредитными картами. После проделывания обычного рода домашней работы, она звонит компании-цели и говорит оператору коммутационной панели, который отвечает, чтобы ее переключили на отдел Телекоммуникаций. Добравшись до отдела Телекоммуникаций, она просит администратора голосовой почты.

Используя информацию, собранную в процессе ее исследований, она объясняет что ее зовут Норма Тодд, она из офиса в Кливленде. Пользуясь уловкой, которая к данному моменту уже должна быть вам знакома, она говорит что она собирается в штабквартиру корпорации на неделю, и что ей потребуется там ящик голосовой почты, так что ей не надо будет делать междугородние звонки для проверки сообщений ее голосовой почты. Нет нужды в физическом телефонном соедине-

нии, говорит она, просто ящик для голосовой почты. Он говорит, что позаботится об этом, перезвонит ей когда все будет готово чтобы передать требуемую информацию.

Соблазнительным голосом она говорит “Я на пути к собранию, могу я перезвонить через час? ”

Когда она перезванивает, он говорит что все готово и передает ей информацию – ее номер расширения и временный пароль. Он спрашивает, занает ли она как сменить паоль к голосовой почте, и она позволяет провести себя по шагам, хотя и знает их, по крайней мере, настолько же хорошо как и он.

“А кстати,” спрашивает она, “какой номер мне надо набрать чтобы проверить свои сообщения из отеля?” Он дает ей номер.

Ширли звонит, меняет пароль, и записывает свое новое исходящее приветствие.

Ширли атакует

До этих пор все это было легким маневром. Теперь же она готова использовать искусство обмана.

Она звонит в службу поддержки потребителей компании. “Я из отдела Финансовых Сборов, в Кливлендском офисе,” говорит она, а потом пускается в уже знакомое оправдание. “Мой компьютер в ремонте, и мне нужна ваша помощь в поиске этой информации.” И она продолжает, предоставляя имя и день рождения человека, чью личность она намеревается украсть. Далее

она перечисляет нужную ей для получения информацию: адрес, девичье имя матери, номер карты, кредитный лимит, доступный кредит, и историю оплаты. “Перезвоните мне на этот номер”, говорит она, предоставляя внутренний номер расширения, который администратор голосовой почты установил для нее. “И если меня не будет, просто оставьте информацию на мою голосовую почту.”

Она остается занятой поручениями на остаток утра, а потом проверяет голосовую почту в полдень. Оно все там, все что она просила. Перед тем как отсоединиться, Ширли стирает исходящее сообщение; было бы небрежным оставить запись ее голоса на том конце.

Воровство личности, самое быстро растущее преступление в Америке, “входящее” преступление нового века, почти обзавелось еще одной жертвой. Ширли использует кредитную карту и инфомацию о личнсти которую она только что получила, и начинает накручивать расходы на карту жертвы.

Анализ обмана

В этой уловке атакующая сначала одурачила администратора голосовой почты компании, заставляя поверить что она сотрудник компании, так что он установил временный ящик для голосовой почты. Если бы он вообще побеспокоился проверить, он бы обнаружил что имя и номер телефона которые она дала совпадают со списком в базе данных корпорации.

Остальное было просто делом предъявления разумного оправдания о компьютерной проблеме, требованием нужной информации, и запросом оставить ответ на голосовой почте. Да и зачем бы это любому сотруднику сопротивляться, не делясь информацией с коллегой? Так как телефонный номер, который Ширли предоставила, был сугубо внутренним расширением, то не было и причины для любого подозрения.

Сообщение от Митника

Попробуйте изредка названивать на вашу собственную голосовую почту; если вы услышите исходящее сообщение и оно не ваше, может вы только что наткнулись на вашего первого социального инженера.

Полезный секретарь

Взломщик Роберт Джордэй регулярно вламывался в компьютерные сети компании мирового уровня Rudolfo Shipping, Inc. Компания в конце концов распознала, что кто-то занимается хакингом на их терминальном сервере, и происходит это через тот сервер, через который пользователь может присоединиться к любой компьютерной системе в компании. Чтобы обезопасить корпоративную сеть, компания решила требовать пароль дозвона на каждом терминальном сервере.

Роберт позвонил в Центр Сетевых Операций, позируя адвокатом из Юридического Отдела и сказал, что у него неприятности с присоединением к сети. Сетевой администратор, до которого он дозвонился, объяснил что недавно там были некоторые неувязки с безопасностью, так что всем пользователям с доступом по дозвону необходимо получить ежемесячный пароль у их менеджера. Роберт интересовался что за метод использовался для передачи ежемесячного пароля менеджеру, и как он мог его получить. Обернулось тем, что ответ был таков: пароль для следующего месяца посылался в деловой записке через офисную почту каждому менеджеру компании.

Это все упрощало. Роберт провел мальнькое иссле-

дование, позвонил в компанию сразу после первого числа месяца, и дозвонился до секретарши одного менеджера, которая представилась как Джанет. Он сказал, “Джанет, привет. Это Рэнди Голдштейн из отдела Исследований и Разработок. Я знаю я наверное получил записку с паролем этого месяца для залогинивания к терминальному серверу извне компании, но я не могу ее нигде найти. А вы получили вашу записку на этот месяц?”

Да, сказала она, получила.

Он спросил не могла бы она отправить эту записку ему по факсу, и она согласилась. Он дал номер факса секретарши вестибюля в другом здании кампуса компании, где он уже наладил все так чтобы факсы держали для него, и потом собирался устроить пересылку факса с паролем. Однако в этот раз Роберт использовал другой способ пересылки факса. Секретарю он дал номер факса который шел на онлайновую факсовую службу. Когда эта служба получила факс, авоматизированная система переслала его на адрес электронной почты подписчика.

Новый пароль пришел на электронный адрес мертвого сброса почты, который Роберт создал на бесплатной почтовой службе в Китае. Он был уверен, что даже если факс вообще отследили, расследователь рвал бы на себе волосы, пытаясь наладить сотрудничество с официальными лицами в Китае, которые, как он знал,

более чем противились помогать в подобных делах. Лучшее из всего, ему вообще не надо было физически показываться в месте расположения факс-машины.

Сообщение от Митника

Искусный социальный инженер очень умен в побуждении других людей делать ему одолжения. Получение факса и перенаправление его в другое место выглядит настолько безобидно, что все это слишком просто убедить секретаря или кого-нибудь еще согласиться сделать это.

Суд по делам дорожного движения

Наверное каждый, кто получал квитанцию штрафа за превышение скорости, наиву мечтал о каком-нибудь способе это преодолеть. Но не хождением в школу дорожного движения, или просто расплачиваясь по указанной сумме, или получить шанс убедить судью о некоей техничноской стороне дела вроде того, как много времени прошло с тех пор как спидометр полицейской машины или радарная пушка были сверены. Нет, милейшим сценарием было бы победить квитанцию, перехитрив систему.

Жулик

Хотя я бы и не рекемомендовал пробовать этот метод аннулирования квитанции за превышение скорости (по ходу разговора, не пробуйте это в домашних условиях), все же это хороший пример того, как искусство обмана может быть использовано а помощь социальному инженеру.

Давайте будем звать этого нарушителя трафика Полом Дьюриа.

Первые шаги

“Полиция Лос Анжелеса, подразделение Холлэнбек.”

“Здравствуйте, я бы хотел поговорить с отделом

Управления по повесткам в суд.”
“Я судебный пристав.”
“Хорошо. Это адвокат Джон Лилэнд, из адвокатской фирмы Мичем, Мичем и Тэлботт. Мне нужно вызвать в суд офицера по данному делу.”
“О’кей, какого офицера?”
“В вашем подразделении есть офицер Кендэлл?”
“Какой у него порядковый номер?”
“ 21349.”
“Да. Когда он вам нужен?”
“В какое-нибудь время в следующем месяце, но мне еще нужно вызвать нескольких других свидетелей по делу и затем поставить в известность суд какие дни будут для нас удобны. Есть ли какие-нибудь дни когда офицера Кендэлла нельзя будет застать?”
“Давайте посмотрим… У него нерабочие дни с 20-го по 23-е, и тренировочные дни с 8-го по 16-е.”
“Благодарю. Это все что мне было нужно прямо сейчас. Я перезвоню когда дата суда будет назначена.”
Муниципальный суд, Стойка Пристава
Пол: “Я бы хотел наметить дату суда по этой квитанции за превышение скорости.”
Пристав: “О’кей. Я могу дать вам 26-е следующего месяца.”
“Ну я бы хотел запланировать привлечение к суду (освидетельствование).”
“Вы хотите привлечение к суду по квитанции за пре-

вышение скорости?”

“Да.”

“О’кей. Мы можем назначить слушание завтра утром или в полдень. Что бы вы хотели?”

“Полдень.”

“Слушание завтра в 13:30 в Комнате для судебных заседаний номер шесть.”

“Спасибо. Я буду там.”

Муниципальный Суд, Комната для судебных заседаний номер шесть

Дата: Четверг, 13:45

Пристав: “М-р Дьюреа, пожалуйста займите место на скамье.”

Судья: “М-р Дьюреа, вы понимаете права, объясненные Вам в этот полдень?”

Пол: “Да, Ваша честь.”

Судья: “Вы хотите использовать возможность посещения школы дорожного движения? Ваше дело будет отменено после завершения восьмичасового курса. Я проверил Ваше дело и Вы вполне имеете право.”

Пол: “Нет, Ваша честь, я со всем уважением прошу чтобы дело было переведено на испытательный срок. И еще одна вещь, Ваша честь, я собираюсь в путешествие за пределы страны, но я свободен 8-го и 9-го. Может ли быть возможным поставить мое дело на испытательный срок также и на эти дни? Я уезжаю в деловую поездку в Европу завтра, и вернусь через четы-

ре недели.”

Судья: “Очень хорошо. Испытание назначено на 8-е Июня, 8:30 утра, Комната для судебных заседаний номер четыре.”

Пол: “Благодарю Вас, Ваша честь.”

Муниципальный Суд, Комната для судебных заседаний номер четыре

Пол прибыл в суд 8-го числа рано. Когда судья вошел, пристав дал ему список дел, на которые офицер не явился. Судья вызвал ответчиков, включая Пола, и сказал им что их дела расформированы.

Анализ обмана

Когда офицер выписывает билет, он подписывает его своим именем и символическим номером(или каким угодно еще, как зовется его персональный номер в его агентсве). Звонка ассистенту справочной с указанием названия законо-принудительного учреждения указанного на ссылке (дорожно-патрульная служба, шериф округа, или что угодно еще) достаточно, чтобы просунуть ногу в дверь. Как только связь с агенством установлена, они могут отослать звонящего на верный телефонный номер судебного пристава, обслуживающего географическую зону где остановка за нарушение движения была совершена.

Офицеры,занимающиеся привлечением к ответственности перед законом, вызываются в суд регулярно; это зависит от территории. Когда окружному ад-

вокату или юристу защиты требуется освидетельствовать офицера, если они знают как работает система, они первым делом для уверенности проверяют, будет ли офицер доступен. Это сделать просто; требуется всего лишь звонок судебному приставу того агентства.

Обычно в таких беседах адвокат спрашивает, будет ли офицер доступен в такую-то и такую-то дату. Для этой же уловки Полу требовалось немного такта; он должен был предложить правдоподобную причину почему пристав должен сказать в какие даты офицера *не будет* .

Когда он впервые пришел в здание суда, почему Пол просто не сказал судебному приставу какая дата ему нужна? Проще простого – насколько я понимаю, судебные приставы по дорожным происшествиям в большинстве мест не позволяют общественности выбирать судебные даты. Если дата, которую пристав предложил, не устраивает человека, она(пристав) предлагает одну или две альтернативных, но это настолько, насколько она будет склонна к этому. С другой стороны, любому, кто желает получить дополнительное время на явку для привлечения к суду, вероятно удача будет сопутствовать лучше.

Пол знал, что он имел право просить о привлечении к суду. И он знал что судьи часто желают согласовывать запрос на специфическую дату. Он тщательно расспросил по поводу дат, которые совпадают с трени-

ровочными днями офицера, зная что в его положении офицерские тренировки берут приоритет перед явкой в дорожный суд.

Сообщение от Митника

Человеческий разум – чудное создание. Интересно отмечать насколько сообразительными могут быть люди в отработке обманных путей получения того, чего они хотят, или чтобы выбраться из неприятной ситуации. Вы должны использовать такую же находчивость и воображение для охраны информации и компьютерных систем в общесвенном и частном секторах. Так что, народ, когда разрабатываете политику безопасности вашей компании – будьте сообразительными и думайте более открыто.

А в дорожном суде когда офицер не является – дело закрыто. Никаких выплат. Никакой школы дорожного движения. Никаких баллов. И, лучшее из всего, никаких записей насчет дорожного нарушения!

Моя догадка, что некоторые официальные лица в полиции, судебные офицеры, районные адвокаты и им подобные будут читать эту историю и качать головой, потому что они знают что эта уловка работает. Но качание головой – это все, что они сделают. Ничего ни изменится. Я бы сделал ставку на это. Как в фильме 1992 года *"Кеды"("Sneakers")* герой Космо говорит, "Все дело в нулях и единицах" – имея ввиду что в конце концов все сводится к информации.

До тех пор, пока законо-принудительные агентства желают раздавать информацию об офицерском расписании виртуально кому угодно, кто им звонит, способность ухода от квитанций будет существовать всегда. А у вас есть похожие прорехи в вашей компании или организационные процедуры, преимуществом которых умный социальный инженер может воспользоваться чтобы получить информацию, которой вы бы предпочли чтобы у него не было?

Возмездие Саманты

Саманта Грегсон была сердита.

Она тяжело работала над ее степенью по бизнесу в колледже, и накопила кипы студенческих займов чтобы заниматься этим. В нее всегда вбивалось, что степень колледжа – это как ты получил карьеру вместо работы, как заработал большие деньги. А потом она окончила колледж и не смогла нигде найти достойную работу.

Как она была рада получить предложение от компании Lambeck Manufacturing. Конечно, было унизительным принимать позицию секретаря, но м-р Кэтрайт сказал как сильно они хотели взять ее, и что принятие секретарской работы засветило бы ее, когда следующая неадминистративная должность будет открытой.

Два месяца спустя она услышала, что один из младших менеджеров по продукции Кэтрайта собирался уходить. Она с трудом могла уснуть в ту ночь, представляя себя на пятом этаже, в офисе с дверью, посещая собрания и принимая решения.

На следующее утро она первым делом пошла повидать м-ра Кэтрайта. Он сказал, что им кажется ей следовало бы побольше узнать об индустрии перед тем как она будет готова для профессиональной должно-

сти. А потом они пошли и наняли новичка за пределами компании, который знал об индустрии меньше нее.

Это было как раз перед тем, как до нее стало доходить: в компании было много женщин, но почти все они были секретаршами. Они и не собирались давать ей менеджерскую работу. Вообще никогда.

Расплата

Ей потребовалась около недели чтобы выяснить как она собирается им отплатить. Месяцем ранее парень из журнала индустриальной торговли попытался запасть на нее когда пришел на запуск нового продукта. Несколькими неделями спустя он позвонил ей на работу и сказал, что если бы она прислала некоторую дополнительную информацию на продукт с названием Cobra 273, он бы прислал ей цветы, а если бы это была на самом деле горячая информация, которую он мог бы использовать в журнале, он бы специально приехал из Чикаго просто чтобы пойти с ней поужинать.

Она побывала в офисе молодого м-ра Джоэнссена буквально через день после того, как он имел доступ(залогинивался) к корпоративной сети. Не раздумывая, она проследила за его пальцами (“*плечевой серфинг* ”, как это иногда называется). Он ввел “marty63” в качестве своего пароля.

В ее плане все начинало сходиться. Была записка которую она, как она вспомнила, печатала немногим позденее ее прихода в компанию. Она нашла копию в

файлах и напечатала новую версию, используя язык исходной. Ее версия читалась так:

КОМУ: К. Пелтон, отдел Информационных Технологий

ОТ: Л. Кэтрайт, отдел Разработок

Мартин Джоэнссен будет работать в команде специальных проектов в моем отделе.

Тем самым я авторизую его для получения доступа к серверам, используемым инженерной группой. Профиль безопасности м-ра Джоэнссена будет обновлен для предоставления ему тех же прав доступа, как и у разработчика продукта.

Луис Кэтрайт

LINGO

ПЛЕЧЕВОЙ СЕРФИНГ Акт наблюдения за тем, как человек печатает на клавиатуре своего компьтера, с тем чтобы обнаружить и украсть его пароль или другую пользовательскую информацию.

Когда почти все ушли на ланч, она вырезала подпись м-ра Кэтрайта из оригинальной(исходной) записки, вклеила ее в новую версию, и намалевала канцелярским корректором по краям. Она сделала копию с результата, а потом сделала копию с копии. Вы бы едва смогли различить кромки вокруг подписи. Она послала факс с машины неподалеку от офиса м-ра Кэтрайта.

Три дня спустя она осталась внеурочно и подождала пока все уйдут. Она вошла в офис Джоэнссена и по-

пробовала залогиниться в сеть с его именем пользователя и паролем, marty63. Это сработало.

В считанные минуты она обнаружила файлы спецификации продукта Cobra 273, и скачала их на Zip-диск.

Диск надежно был в ее кошельке когда она вышла на прохладный ночной ветерок на парковочной стоянке. Диск был на своем пути к репортеру в тот вечер.

Анализ обмана

Недовольный сотрудник, поиск среди файлов, быстрая операция вырезки-вставки-и-коррекции, немного творческого копировая, и факс. И, вуаля! – у нее есть доступ к конфиденциальным спецификациям на маркетинг и продукт.

И спустя несколько дней, у журналиста из журнала по торговле есть большой ковш со спецификациями и маркетинговыми планами нового горячего продукта, который будет в руках подписчиков журнала по всей индустрии месяцами ранее выпуска продукта. У компаний-конкурентов будет несколько месяцев наперед, чтобы начать разрабатывать эквивалентные продукты и держать их рекламные кампании наготове, чтобы подорвать Cobra 273.

Естественно, журнал никогда не расскажет, где они взяли зацепку.

Предотвращение обмана

Когда спрашивают любую ценную, чувствительную, или критически важную информацию, которая может сослужить выгоду конкуренту или кому угодно еще, сотрудники должны быть осведомлены, что использование услуги “caller ID” в смысле подтверждения личности звонящего извне недопустимо. Некоторые другие средства подтверждения должны быть использованы, такие как сверка с куратором того человека по поводу того, что запрос был соответствующим, и что у пользователя есть авторизация для получения информации.

Процесс проверки требует балансировочного акта, который каждая компания должна определить для себя: безопасность против продуктивности. Какой приоритет будет назначен для усиления мер безопасности? Будут ли сотрудники сопротивляться следованию процедур безопасности, и даже обходить их в порядке дополнения к их рабочим обязанностям? Понимают ли сотрудники почему безопасность важна для компании и для них самих? На эти вопросы должны быть найдены ответы чтобы разработать политику безопасности, основанную на корпоративной культуре и деловых нуждах.

Большинство людей неизбежно видят досаду во

всем, что пересекается с выполнением их работы, и могут обойти любые меры безопасности, которые кажутся пустой тратой времени. Мотивировать сотрудников сделать безопасность частью их повседневных обязанностей через обучение и осведомленность – это и есть ключ.

И хотя сервис “caller ID” никогда не должен использоваться в смысле аутентификации для голосовых звонков извне компании, другой метод, называемый Автоматическим Определением Номера (АОН – Automated Number Identification, ANI), может. Эта услуга предоставляется когда компания подписывается на бесплатные услуги, где компания платит за исходящие звонки и надежна для идентификации. В отличие от “caller ID”, коммутатор телефонной компании не использует любого рода информацию, которая посылается от потребителя когда предоставляется номер вызывающего. Номер, передаваемый АОН’ом, является оплачиваемым номером, назначенным звонящей стороне.

Заметьте, что несколько изготовителей модемов добавили функцию “caller ID” в их продукты, защищая корпоративную сеть путем дозволения звонков удаленного доступа только из списка заранее авторизованных телефонных номеров. Модемы с “caller ID” – дупустимая мера аутентификации в низко-безопасном окружении, но, как уже должно быть ясно, подмена caller ID – относительно простая техника для компью-

терных злоумышленников, и поэтому не должна служить опорой для подтверждения личности звонящего или местнонахождения в обстановке высокой безопасности.

Чтобы адресовать случай с воровством личности, как в истории с обманом администратора для создания ящика голосовой почты на корпоративной телефонной системе, сделайте такую политику, чтобы весь телефонный сервис, все ящики голосовой почты, и все записи в корпоративный справочник, обоих видов – печатные и онлайновые – должны быть запрошены в письменном виде, на бланке/форме по назначению. Менеджер сотрудника должен подписать запрос, а администратор голосовой почты должен проверить подпись.

Корпоративная политика безопасности должна требовать, чтобы все компьютерные аккаунты или повышения прав доступа предоставлялись только после положительной верификации персоны, осуществляющей запрос, такими путями, как перезвон системному менеджеру или администратору, или его/ее поверенному, по телефонному номеру, указанному в печатном или онлайновом справочнике. Если компания использует защищенную электронную почту, где сотрудники могут подписывать сообщения Электронной Цифровой Подписью, такой альтернативный метод верификации тоже может быть допустимым.

Помните, что каждый сотрудник, независимо от того имеет ли он доступ к компьютерным системам компании, может стать жертвой обмана социального инженера. Каждый должен быть включен в тренинги осведомления о безопасности. Асситенты администратора, регистраторы, телефонные операторы и охранники должны быть знакомы с теми типами атак социального инжениринга, которые более вероятно будут направлены против них, так что они будут лучше подготовлены к защите от этих атак.

Глава 14: Промышленный шпионаж

Будет опубликована в ближайшее время.

Глава 15: Знание об информационной безопасности и тренировки

Перевод: sly (**http://slyworks.net.ru**) icq:239940067

Социальный инженер задумал заполучить проект (исходники) Вашего нового продукта за 2 месяца до релиза.

Что остановит его?

Ваш файервол? Нет.

Мощная система идентификации? Нет.

Система обнаружения вторжений? Нет.

Шифрование данных? Нет.

Ограничение доступа к номерам дозвона модемов? Нет.

Кодовые имена серверов, которые затрудняют определение местонахождения проекта искомого продукта? Нет.

Смысл здесь в том, что никакая технология в мире не сможет противостоять атаке социального инженера.

Обеспечение безопасности с помощью технологии, тренировки и процедуры

Компании, которые проводят тесты на возможность проникновения, сообщают, что их попытки проникнуть в компьютерную систему компании с помощью методов социнженерии практически в *100% случаев* удаются. Технологии безопасности могут усложнить этот тип атак путем исключения людей из процесса принятия решений. Тем не менее истинно эффективный путь ослабить угрозу социальной инженерии можно через использование технологий безопасности, комбинированных с политикой безопасности, которая устанавливает правила поведения служащих, а также *включающих* обучение и тренировку сотрудников.

Единственный путь сохранить разработки Вашего продукта нетронутыми – иметь тренированную, знающую и добросовестную рабочую команду. Это подразумевает тренировку с использованием политик и процедур, но, вероятно, более важным является переход к программе распределенной осведомленности. Некоторые компании, занимающиеся вопросами безопасности, рекомендуют тратить на тренировку таких программ до 40% бюджета компании.

Первый шаг – приучить каждого на предприятии к мысли, что существуют бессовестные люди, которые могут с помощью обмана и психологии манипулировать ими. Служащие должны знать, какая информация нуждается в защите, и как эту защиту осуществлять. Однажды хорошо прочувствовав и поняв, как можно поддаться чужим манипуляциям, они будут находиться в намного более выгодной позиции, чтобы распознать атаку.

Осведомление о безопасности включает также обучение каждого работающего в компании политикам и процедурам. Как обсуждается в главе 17, политики – это необходимые и обязательные правила, которые описывают поведение сотрудников для защиты корпоративной информационной системы и особо ценной информации.

Эта и следующая главы показывают безопасный шаблон (blueprint – синька, светокопия), который обезопасит Вас от атак, которые дорого могут Вам обойтись. Если Вы не тренируете персонал, следующий процедурам обработки информации (well– thought —out procedures), это до *того* момента, *пока* Вы не потеряете информацию благодаря социальному инженеру. Не тратьте время, ожидая атак, которые могут случиться, пока решаете, разрабатывать или не разрабатывать политики безопасности: они могут разорить Ваш бизнес и разрушить благополучие Ваших рабочих.

Понимание того, как атакующий может воспользоваться человеческой природой

Для того, чтобы разработать действенную программу обучения, Вы должны понять, почему люди в первую очередь уязвимы для атак. Для выделения этих тенденций в вашей программе, например, обратить на них внимание благодаря дискуссии – этим Вы поможете сотрудникам понять, как социальный инженер может манипулировать людьми.

Манипуляция начала изучаться социальными исследователями в последние 50 лет. Robert B. Cialdini, написавший в *«Американской науке»* (Февраль 2001), объединил результаты этих исследований и выделил 6 «черт человеческой натуры», которые используются в попытке получения нужного ответа.

Это 6 приемов, которые применяются социальными инженерами наиболее часто и успешно в попытках манипулировать.

Авторитетность

Людям свойственно желание услужить (удовлетворить запрос) человеку с авторитетом (властью). Как говорилось раньше, человек получит нужный ответ, если сотрудник уверен, что спрашивающий имеет власть

или право задавать этот вопрос.

В своей книге *«Влияние»* Dr. Cialdini написал об обучении в 3 госпиталях Мидвестерна, в которых аппараты 22 медсестер соединялись с человеком, который выдавал себя за физиотерапевта, инструктируя административный персонал на выписку рецепта препарата (наркотика?) пациенту. Медсестры, которые получили это указание, не знали звонившего. Они не знали, действительно ли он доктор (а он им не был). Они получали инструкции для выписки рецепта по телефону, что нарушает политику безопасности госпиталя. Препарат, который указывался, не разрешен к применению, а его доза составляла в 2 раза большую, чем допустимая суточная норма – все это может опасно отразиться на состоянии здоровья пациента или даже убить его. Более чем в 95% случаев Cialdini сообщает, что «медсестра брала необходимую дозу из палаты с медикаментами и уже была на пути к палате указанного пациента», где перехватывалась наблюдателем, который сообщал ей об эксперименте.

Примеры атак:

Социнженер пытается выдать себя за авторитетное лицо из IT департамента или должностное лицо, выполняющее задание компании.

Умение расположить к себе

Люди имеют привычку удовлетворить запрос располагающего к себе человека, или человека со сходными

интересами, мнением, взглядами, либо бедами и проблемами.

Примеры атак:

В разговоре атакующий пытается выяснить увлечения и интересы жертвы, а потом с энтузиазмом сообщает, что все это ему близко. Также он может сообщить, что он из той же школы, места, или что-то похожее. Социальный инженер может даже подражать цели, чтобы создать сходство, видимую общность.

Взаимность

Мы можем машинально ответить на вопрос, когда получаем что-то взамен. Подарком в этом случае может служить материальная вещь, совет или помощь. Когда кто-то делает что-то для нас, мы чувствуем желание отплатить. Эта сильная черта человеческой натуры проявляется тогда, когда получивший подарок не ждал (не просил) его. Один из самых эффективных путей повлиять на людей, чтобы получить благосклонность (расположить к себе, а, следовательно, получить информацию) – преподнести неявно обязывающий подарок.

Поклонники религиозного культа Хари Кришны очень опытны в умении получать влияние над человеком путем преподнесения подарка – книги или цветка. Если человек пробует вернуть, отказаться от подарка, дарящий мягко настаивает: «Это наш подарок Вам». Этот основной принцип взаимности использо-

вался Кришнами для постоянного увеличения пожертвований.

Примеры атак:

Сотрудник получает звонок от человека, который называет себя сотрудником IT департамента. Звонящий рассказывает, что некоторые компьютеры компании заражены новым вирусом, который не обнаруживается антивирусом. Этот вирус может уничтожить (повредить) все файлы на компьютере. Звонящий предлагает поделиться информацией, как решить проблему. Затем он просит сотрудника протестировать недавно обновленную утилиту, позволяющую пользователю сменить пароли. Служащему неудобно отказать, потому что звонящий лишь предлагает помощь, которая защитит пользователей от вируса. Он хочет отплатить, сделав что-нибудь для «доброго человека». Например, ответить на пару вопросов…

Ответственность

Люди меют привычку исполнять обещанное. Раз пообещав, мы сделаем все, потому что не хотим казаться не заслуживающими доверия. Мы будем стремиться преодолеть любые препятствия для того, чтобы сдержать слово или выполнить обязанность.

Примеры атак:

Атакующий связывается с подходящим новым сотрудником и советует ознакомиться с соглашением о политиках безопасности и процедурах, потому что это

– основной закон, благодаря которому можно пользоваться информационными системами компании. После обсуждения нескольких положений о безопасности атакующий просит пароль сотрудника «для подтверждения согласия» с соглашением. Он должен быть сложным для угадывания. Когда пользователь выдает свой прароль, звонящий дает рекомендации, как выбирать пароли в следующий раз, чтоб взломщикам было сложно подобрать их. Жертва соглашается следовать советам, потому что это соответствует политике компании. К тому же рабочий предполагает, что звонивший только что подтвердил его согласие следовать соглашению.

Социальная принадлежность к авторизованным

Людям свойственно не выделяться в своей социальной группе. Действия других являются гарантом истинности в вопросе поведения. Иначе говоря, «если так делают другие, я тоже должен действовать так».

Примеры атак:

Звонящий говорит, что он проверяющий и называет имена других людей из департамента, которые занимаются проверкой вместе с ним. Жертва верит, потому что остальные названные имена принадлежат работникам департамента. Затем атакующий может задавать любые вопросы, вплоть до того, какие логин и пароль использует жертва.

Ограниченное количество «бесплатного сыра»

Еще одна из потенциально опасных для безопасностии информации человеческих черт – вера в то, что объект делится частью информации, на которую претендуют другие, или что эта информация доступна только в этот момент.

Примеры атак:

Атакующий рассылает электронные письма, сообщающие, что первые 500 зарегистрировавшихся на новом сайте компании выиграют 3 билета на премьеру отличного фильма. Когда ничего не подозревающий сотрудник регистрируется на сайте, его просят ввести свой адрес электронного почтового ящика на рабочем месте и выбрать пароль. Многие люди, чтоб не забыть множество паролей, часто используют один и тот же во всех системах. Воспользовавшись этим, атакующий может попытаться получить доступ к целевому рабочему или домашнему компьютеру зарегистрировавшегося.

Создание тренировочных и образовательных программ

Выпуская брошюру политик информационной безопасности или направляя рабочих на Интранет-страницу с этими правилами, но которая не содержит простого разъяснения деталей, вы уменьшаете риск. Каждый бизнес должен не только иметь прописные правила, но и побуждать (заставлять) старательно изучить и следовать этим правилам *всех* , кто работает с корпоративной информацией или компьютерной системой. Более того, вы должны убедиться, что все понимают причину принятия того или иного положения этих правил, поэтому они не попытаются обойти эти правила ради материальной выгоды. Иначе незнание всегда будет отговоркой рабочих и совершенно точно, что социальный инженер воспользуется этим незнанием.

Главная цель любой обучающей программы состоит в том, чтобы заставить людей сменить их поведение и отношение, мотивировать их желание защитить и сохранить свою часть информации организации. Хорошим мотивом тут будет демонстрация того, как за их участие будет вознаграждена не сама компания, а конкретные сотрудники. Начиная с того момента, когда компания начнет сохранять определенную персональ-

ную информацию о каждом работнике, а рабочие будут выполнять свою часть по защите информации и информационных сетей, то и эта персональная информация будет также надежно сокрыта.

Программа тренировки безопасности требует прочной поддержки. Для тренировочных занятий нужно, чтобы каждый, кто имеет доступ к важной информации или компьютерной информационной системе, не должен быть пассивен, должен постоянно исправляться, совершенствоваться, «натаскивая» персонал на новые угрозы и уязвимости. Это обязательство должно быть реальным делом, а не пустой отговоркой «ну и Бог с ним». А также программа должна быть подкреплена достаточными ресурсами для разработки, взаимодействия, тестирования – вот чем определяется успех.

Цели

Основным направлением, которого следует придерживаться при разработке программы по тренингу и защите информации, является фокусировка на мысли, что они могут подвергнуться нападению в любое время. Они должны заучить свою роль в защите от любой попытки проникновения в компьютерную систему или кражи важных данных.

Так как многие аспекты информационной безопасности являются «вовлекающей» технологией, то сотрудникам легко представить, что проблема обнару-

жится файерволом или другими средствами защиты. Главная цель здесь – заставить находящихся на ответственных местах сотрудников осознать, как усилить информационную «броню» организации.

Тренинг по безопасности должен быть более важной целью, чем простые правила для ознакомления. Создатель тренинга должен признать сильное желание части сотрудников, которые под давлением желания окончить работу не обратят внимание или проигнорируют обязанности по обеспечению защиты. Знание тактик и приемов социнженерии и пути их предотвращения безусловно важны, но они будут бесполезны без фокусирования создателя тренинга на *мотивации* работников использовать эти знания.

Компания может считать цель достигнутой, если все ее сотрудники свыкнуться с мыслью, что защита информации – часть их работы.

Сотрудники должны прийти к серьезному убеждению, что атаки социальной инженерии реальны, что потеря важной корпоративной информации может угрожать не только компании, но персонально каждому из них, их работе и благосостоянию. Не заботиться об информационной безопасности эквивалентно не заботиться о своем PIN-коде или номере кредитной карты. Эту аналогию можно использовать, чтобы вызвать энтузиазм в тренинге со стороны подчиненных.

Учреждение обучающего тренинга

Ответственный за разработку программы информационной безопасности должен свыкнуться с мыслью, что это не проект «один размер на всех». В некоторой степени данный тренинг нуждается в выработке специфических требований для отдельных групп сотрудников, участвующих в делопроизводстве. В то время как описанные в главе 16 политики безопасности применимы ко всем без исключения работникам, другие уникальны. По минимуму, большинство компаний должно иметь в своем арсенале тренинги для следующих групп персонала: менеджеры, IT-сотрудники, пользователи ПК, обслуживающий персонал, администраторы и их ассистенты, техники связи, охранники. (Смотри деление полиции по роду занятий в главе 16.)

Начнем с персонала отдела технической безопасности: удивительно надеяться на неопытность в компьютерах и на ограниченность его сотрудников, которые не будут, как вам кажется, входить в контакт с другими компьютерами компании и экспериментировать – обычно это упускается из внимания при подготовке программы этого типа. Также социнженер может убедить охрану или другого работника впустить его в здание, или офис, или предоставить доступ, результатом которого станет компьютерное проникновение. Проще говоря – взлом. Пока охранники конечно не нуждаются в прохождении полного курса тренировочной программы, которая необходима персоналу, непосред-

ственно работающему с компьютерами, но и они не-должны быть забыты.

В корпоративном мире существует несколько положений о том, чему должны быть обучены все сотрудники. Они одновременно и важны, и скучны, что присуще безопасности. Действительно хорошая программа по повышению информационной безопасности должна как информировать, так и захватывать внимание, рождать энтузиазм у обучающихся.

Целью должна стать увлекательная, интерактивная программа. Технические приемы обучения должны включать демонстрацию социнженерии с помощью игры по ролям; обзорные медиа-отчеты о последних атаках на других менее удачливых конкурентов и обсуждения путей предотвращения потери информации; просмотр специальных видео-материалов по безопасности, которые непосредственно вводят в курс и обучают одновременно. Такие материалы всегда можно найти в компаниях, занимающихся обеспечением информационной безопасности.

Заметка:

Для тех компаний, которые не имеют средств для самостоятельной разработки программы информационной безопасности существуют компании, предоставляющие данную услугу. Их можно найти на одной из выставочных площадок, например на **http://www.secureworldexpo.com** .

Истории в этой книге представляют собой огромное количество материала для объяснения методов и тактик социальной инженерии, поднятия уровня осведомленности и демонстрации уязвимостей человеческой натуры. Можно полагать, что использование этих историй даст необходимую базу для ролевых игр. Истории также являются яркими темами для оживленных дискуссий о том, как жертвы должны действовать, чтобы предотвратить успешную атаку.

Грамотные разработчики и преподаватели данных тренингов найдут множество трудностей, но также множество возможностей оживить учебный процесс, заставить окружающих стать его частью.

Структура тренинга

В своей основе обучающая программа должна быть спроектирована таким образом, чтобы посещалась всеми сотрудниками. Новые служащие должны посещать тренинг как часть первоначального ознакомления и знакомства с новым местом работы. Я рекомендую вообще не допускать сотрудника до работы с компьютерами, пока он не ознакомится с основами программы информационной безопасности.

Для начала я рекомендую занятие, посвященное внештатным ситуациям и системе оповещений. Пока бОльшая часть материала еще впереди, ознакомление с набором коротких важных сообщений значительно облегчит восприятие на полудневных и полноднев-

ных занятиях, когда людям сложно усвоить такое количество материла.

Особое значение первого занятия будет в выражении особой роли гармонии, которая будет царить в компании, пока все руководствуются данной программой. Более важным, нежели обучающие тренировки, будет мотивация, побуждающая сотрудников принять персональную ответственность за безопасность.

В ситуациях, когда некоторые работники не могут посещать общие занятия, компания должна прибегнуть к иным формам обучения, таким как видео, компьютерные программы, онлайн-курсы или печатные материалы.

После короткого вводного занятия остальные более длинные уроки должны быть спланированы таким образом, чтобы все работники внимательно ознакомились со слабыми местами и техниками атак, которые могут применяться конкретно к ним соответственно занимаемым местам в компании. Необходимо раз в год проводить занятия для повторения и освежения данных правил. Природа угроз и методов использования людей постоянно меняются, поэтому весь материал программы должен постоянно обновляться. Более того, осведомленность и бдительность людей со временем ослабляется, поэтому тренинги должны повторяться через определенные промежутки времени. Особое значение имеет здесь убеждение рабочих в

важности политик безопасности и мотивация следовать им, чем демонстрация специфических угроз и методов социнженерии.

Менеджеры должны бать готовы к трате времени на своих подчиненных, чтобы помочь им вникнуть и самим поучаствовать в процессе обучения. Сотрудники далеко не будут довольны, если им придется посещать занятия в нерабочее время. Это стоит учитывать и при ознакомлении с положениями новых сотрудников – они должны иметь достаточно свободного времени, чтобы освоиться со своими рабочими обязанностями.

Сотрудники, получающие повышение с доступом к важной информации несомненно должны пройти тренинг соответственно их новым обязанностям. Например, когда оператор ПК становится системным администратором, или секретарь переходит на должность ассистента администратора – тренинг необходим.

Содержание тренировочной программы

В своей основе все атаки социнженеров опираются на обман. Жертва руководствуется верой в то, что атакующий – сотрудник или вышестоящий чиновник, авторизованный для получения важной информации, или человек, который вправе инструктировать жертву по работе с компьютером или сопутствующим оборудованием. Почти все эти атаки срываются, если жертва просто делает 2 шага:

Идентификация личности делающего запрос: дей-

ствительно ли он тот, за кого себя выдает?

Авторизован ли этот человек: знает ли он необходимую дополнительную информацию и соответствует ли его уровень доступа сделанному запросу?

Заметка:

Так как одних тренировок недостаточно, используйте технологии безопасности, где только возможно, чтобы создать надежно защищенную систему. Это подразумевает, что безопасность, обеспечиваемая технологиями, измеряется, скорее, действиями отдельно взятых рабочих. Например, когда операционная система настроена на предотвращение закачек программ из Интернета, или когда выбирается короткий, легко отгадываемый пароль.

Если занятия по повышению осведомленности и общего уровня безопасности могут изменить поведение каждого сотрудника, что они будут тщательно проверять каждый запрос, исходя из положений программы. Следовательно, риск подвергнуться атаке социнженера резко падает.

Практическая информация тренинга по безопасности, описывающего черты человеческого характера и связанные с ними аспекты социнженерии, должна включать:

Описание того, как атакующий использует навыки социнженерии для обмана людей.

Описание методов, используемых социнженером

для достижения цели.

Как предупреждать возможные атаки с использованием социальной инженерии.

Процедуру обработки подозрительных запросов.

Куда сообщать о попытках или удачных атаках.

Важность проверки того, кто делает подозрительный запрос, не считаясь с должностью или важностью.

Факт в том, что сотрудники не должны безоговорочно верить кому-то без надлежащей проверки, даже если первым побуждением будет сразу дать ответ.

Важность идентификации и проверки авторизованности кого-либо, кто делает запрос для получения информации или выполнения какого-либо действия с вашей стороны (см. «Процедуры проверки и авторизации», гл. 16, для способов проверки личности).

Процедуры защиты важной информации, включая любые данные для о системе ее хранения.

Положение политик и процедур безопасности компании и их важность в защите информации и корпоративной информационной системы.

Аннотация ключевых политик безопасности и их назначение. Например, каждый работник должен быть проинструктирован, как выбирать сложные для подбора взломщиком пароли.

Обязанности каждого работника следовать политикам и важность «несговорчивости».

Социальная инженерия по определению включает в

себя некоторые виды человеческого взаимодействия. Атакующий будет очень часто использовать разные коммуникационные методы и технологии, чтобы достичь цели. По этой причине полноценная программа осведомленности должна включать в себя:

Политики безопасности для паролей компьютеров и голосовой почты.

Процедуры предоставления важной информации и материалов.

Политику использования электронной почты, включая защиту от удаленных атак с помощью вирусов, червей и «троянов».

Ношение бейджей как метод физической защиты.

Специальные меры в отношении людей, не носящих визиток-бейджей.

Практику использования голосовой почты наиболее безопасным образом.

Классификацию информации и меры для защиты особенно важной.

Установление оптимального уровня защиты для важных документов и медиа-данных, которые ее содержат, а также материалов, содержавших важную, но уже не актуальную, информацию, т.е. архивы.

Также, если компания планирует использовать тестирование с инсценированным проникновением, чтобы проверить свои сильные и слабые места во время атак с использованием социнженерии, то об этом

следует предупредить сотрудников заранее. Дайте им знать, что в любое время может поступить телефонный звонок или запрос любым иным способом, используемым атакующим, который является частью теста. Используйте результаты этого теста не для паники, а для усиления слабых мест в защите.

Детали каждого из этих пунктов будут рассмотрены в главе 16.

Тестирование

Ваша компания может захотеть проверить уровень подготовки сотрудников, приобретенный благодаря тренировочной программе по повышению осведомленности, до того, как их допустят к работе с компьютерной системой. Если тест выстроен последовательно, то множество программ, оценивающих действия сотрудников, помогут выявить и усилить бреши в защите.

Также ваша компания может ввести сертификацию при прохождении данного теста, что будет являться дополнительным и наглядным стимулом для рабочих.

На обязательном завершающем этапе программы следует получить подпись в соглашении следовать установленным политикам и принципам поведения от каждого служащего. Ответственность, которую *каждый* берет на себя, подписав соглашение, помогает избегать в работе сомнений – поступить, как просят, или как установлено политикой безопасности.

Поддержание бдительности

Большинство людей знает, что интерес к обучению даже важным навыкам потухает со временем, разгораясь периодически. Поэтому жизненно важно поддерживать интерес сотрудников к изучению предмета безопасности и защиты от атак постоянно.

Один из методов сохранять безопасность основой мышления работника заключается в том, чтобы сделать информационную безопасность своеобразной работой, обязанностью каждого на производстве. Это ободряет сотрудника, потому что он чувствует себя одной из частей слаженного механизма безопасности компании. С другой стороны здесь существует сильная тенденция «безопасность – не моя работа, мне за нее не платят».

Если основная ответственность за информационную программу безопасности, обычно лежит на сотруднике отдела безопасности или отдела информационных технологий, то разработку такой системы лучше вести совместно со специальным отделом проведения тренинга.

Программа по поддержанию бдительности должна быть как можно более интерактивной и использовать любые доступные каналы для передачи сообщений,

помогающих сотрудникам постоянно помнить о хороших привычках безопасности. Методы должны использовать все доступные традиционные каналы + особенные способы, которые разработчики программ только смогут придумать. К примеру, реклама, юмор и вредные советы – традиционные способы. Использование различных слов и написаний одних и тех же сообщений-напоминаний предохраняет их от назойливости и последующего игнорирования.

Список возможных действий для выполнения этой программы может включать:

Предоставление копий этой книги всем сотрудникам.

Информационные статьи, рассылки, напоминания, календари и даже комиксы.

Публикацию наиболее надежного работника месяца.

Специальные плакаты в рабочих помещениях.

Доски объявлений.

Печатные вкладыши в конвертах с зарплатой.

Рассылки с напоминаниями по электронной почте.

Хранители экрана и экранные заставки с напоминаниями.

Вещание напоминаний через голосовую почту.

Специальные наклейки на телефонах. Например: «Звонящий действительно тот, за кого себя выдает?»

Системные сообщения в компьютерной сети. При-

мер: при входе в систему под своим логином пользователь видит сообщение: «Если Вы пересылаете конфиденциальную информация по Email, не забудьте зашифровать ее!»

Постановку вопроса безопасности одним из постоянных на собраниях, пятиминутках и т.д.

Использование локальной сети для напоминаний в картинках, анекдотах и в виде любой другой информации, которая сможет заинтересовать пользователя и прочитать текст.

Электронные табло в общественных местах, например, в кафетерии, с часто обновляемой информацией о положениях политик безопасности.

Распространение буклетов и брошюр.

Изобретение трюков, таких как печения с предсказаниями с напоминаниями о безопасности вместо загадочных слов о будущем.

Вывод: напоминания должны быть своевременными и постоянными.

«Зачем мне все это?»

Для расширения тренинга я рекомендую активную яркую программу вознаграждений. Вы должны объявлять сотрудникам, кто отличился, выявив и предотвратив атаку социнженера или добился большого успеха в освоении программы безопасности и осведомленности. Существование такой программы поощрения должно подчеркиваться на каждом мероприятии, посвященном тренингу, а взломы должны быть широко освещены и разобраны внутри компании.

Но есть и другая сторона монеты: люди должны понимать, что нарушение политик безопасности и установленных процедур, халатность наказуемы. Все мы делаем ошибки, но взломы не должны повторяться.

Краткое описание безопасности в организации

Перевод: Daughter of the Night (admin@mitnick.com.ru)

Следующие списки и таблицы предоставят сжатую памятку методов, используемых социальными инженерами, подробно описанных в главах с 2 по 14, и процедур подтверждения личности, описанных в главе 16. Модифицируйте эту информацию для вашей организации, сделайте ее доступной, чтобы для ваши сотрудники пользовались ей в случае возникновения вопросов по безопасности.

Определение атаки

Эти таблицы помогут вам обнаружить атаку социального инженера.

Действие

ОПИСАНИЕ

Исследование

Может включать в себя ежегодные отчеты, брошюры, открытые заявления, промышленные журналы, информацию с вэб-сайта. А также выброшенное в помойки.

Создание взаимопонимания и доверия

Использование внутренней информации, выдача себя за другую личность, называние имен людей, знакомых жертве, просьба о помощи, или начальство.

Эксплуатация доверия

Просьба жертве об информации или совершении действия. В обратной социальной инженерии, жертва просит атакующего помочь.

Применение информации

Если полученная информация – лишь шаг к финальной цепи, атакующий возвращается к более ранним этапам, пока цель не будет достигнута.

Типичные методы действий социальных инженеров

Представляться другом-сотрудником

Представляться сотрудником поставщика, партнерской компании, представителем закона

Представляться кем-либо из руководства

Представляться новым сотрудником, просящим о помощи

Представляться поставщиком или производителем операционных систем, звонящим, чтобы предложить обновление или патч.

Предлагать помощь в случае возникновения проблемы, потом заставить эту проблему возникнуть, принуждая жертву попросить о помощи

Отправлять бесплатное ПО или патч жертве для установки

Отправлять вирус или троянского коня в качестве приложения к письму

Использование фальшивого pop-up окна, с просьбой аутентифицироваться еще раз, или ввести пароль

Записывание вводимых жертвой клавиш компьютером или программой

Оставлять диск или дискету на столе у жертвы с вредоносным ПО

Использование внутреннего сленга и терминологии для возникновения доверия

Предлагать приз за регистрацию на сайте с именем пользователя и паролем

Подбрасывать документ или папку в почтовый отдел

компании для внутренней доставки

Модифицирование надписи на факсе, чтобы казалось, что он пришел из компании

Просить секретаршу принять, а потом отослать факс

Просить отослать документ в место, которое кажущееся локальным

Получение голосовой почты, чтобы работники, решившие перезвонить, подумали, что атакующий – их сотрудник

Притворяться, что он из удаленного офиса и просит локального доступа к почте.

Предупреждающие знаки атаки

Отказ назвать номер

Необычная просьба

Утверждение, что звонящий – руководитель

Срочность

Угроза негативными последствиями в случае невыполнения

Испытывает дискомфорт при опросе

Называет знакомые имена

Делает комплименты

Флиртует

Типичные цели атакующих

ТИП ЖЕРТВЫ

ПРИМЕРЫ

Незнающая о ценности информации

Секретари, телефонистки, помощники администра-

ции, охрана.

Имеющая особенные привилегии

Отдел технической поддержки, системные администраторы, операторы, администраторы телефонных систем.

Поставщик/ Изготовитель

Производители компьютерных комплектующих, ПО, поставщики систем голосовой почты.

Особый отдел

Бухгалтерия, отдел кадров.

Факторы, делающие компанию более уязвимой к атакам

Большое количество работников

Множество филиалов

Информация о местонахождении сотрудников на автоответчике

Информация о внутренних телефонах общедоступна

Поверхностное обучение правилам безопасности

Отсутствие системы классификации информации

Отсутствие системы сообщения об инцидентах

Проверка и классификация информации

Эти таблицы и списки помогут вам ответить на просьбы или действия, которые могут быть атакой социального инженера.

Подтверждение личности

ДЕЙСТВИЕ

ОПИСАНИЕ

Идентификационный номер звонящего

Убедитесь, что звонок– внутренний, и название отдела соответствует личности звонящего.

Перезвонить

Найдите просящего в списках компании и перезвоните в указанный отдел.

Подтвердить

Попросите доверенного сотрудника подтвердить личность просящего.

Общий секрет

Спросите известный только в фирме секрет, к примеру пароль или ежедневный код.

Руководитель или менеджер

Свяжитесь с руководителем сотрудника и попросите подтвердить личность и должность.

Безопасная почта

Попросите отправить сообщение с цифровой подписью.

Узнавание голоса

Если звонящий знаком, убедитесь, что это его голос.

Меняющиеся пароли

Спросите динамический пароль вроде Secure ID, или другое аутентификационное средство.

Лично

Попросить звонящего прийти с удостоверением личности.

Проверка, работает ли еще сотрудник

ДЕЙСТВИЕ

ОПИСАНИЕ

Проверка в списке сотрудников

Проверьте, что сотрудник находится в списке.

Менеджер просителя

Позвонить менеджеру просителя используя телефон, указанный в базе данных компании.

Отдел или группа просителя

Позвонить в отдел просителя и узнать, работает ли он еще там.

Процедура, позволяющая узнать, может ли просителя получить информацию

ДЕЙСТВИЕ

ОПИСАНИЕ

Смотреть список должностей / отделов / обязанностей

Проверить списки, где сказано, каким сотрудникам разрешено получать подобную информацию.

Получить разрешение от менеджера

Связаться со своим менеджером или менеджером звонящего для получения разрешения выполнить просьбу.

Получить разрешение от владельца информации или разработчика

Спросить владельца информации, надо ли звонящему это знать.

Получить разрешение от автоматического устройства

Проверить базу данных уполномоченного персонала.

Критерии подтверждения личности людей, не являющихся сотрудниками

КРИТЕРИИ

ДЕЙСТВИЕ

Связь

Убедитесь, что у фирмы просителя есть поставщики, партнеры или другие соответствующие связи.

Личность

Проверьте личность и статус занятости звонящего в его фирме.

Неразглашение

Убедитесь, что просителя подписал договор о неразглашении тайн.

Доступ

Передайте просьбу руководству, если информация классифицирована секретней, чем «Внутренняя».

Классификация информации

КЛАССИФИКАЦИЯ

ОПИСАНИЕ

ПРОДЕДУРА

Публичная

Может быть свободно доступна для общественного пользования.

Не требует подтверждения личности

Внутренняя

Для использования внутри компании

Проверьте, является ли просящий сотрудником в данный момент, подписал ли он соглашение о неразглашении, и попросите разрешение руководства для людей, не являющихся сотрудниками.

Личная

Информация личного характера,

предназначенная для использования только внутри организации.

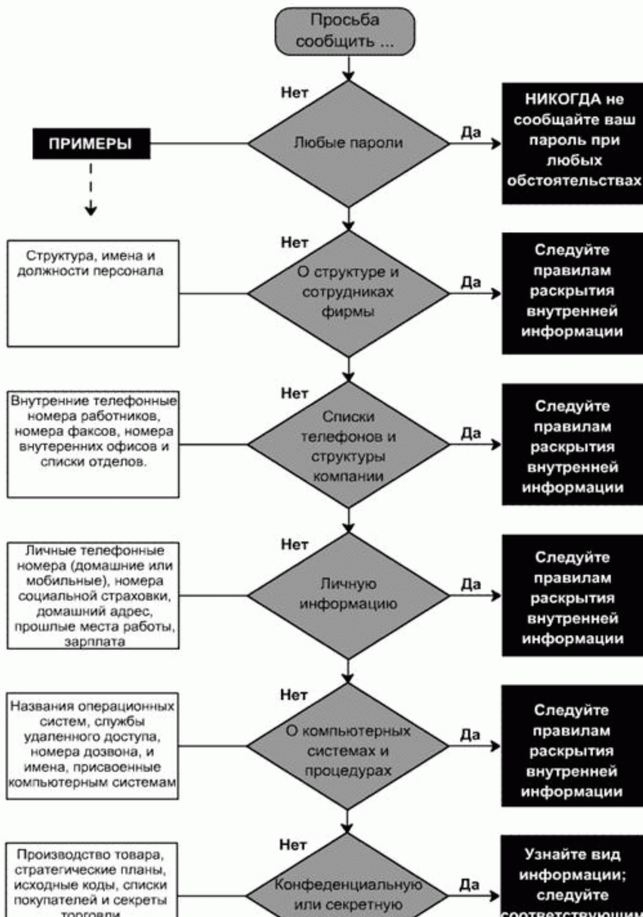
Проверьте, является ли просителя сотрудником в данный момент, или у него есть разрешение. Свяжитесь с отделом кадров насчет раскрытия информации сотрудникам или людям, не являющихся сотрудниками.

Конфиденциальная

Известна только людям, которым необходимо это знать внутри организации.

Подтвердите личность звонящего и спросите у владельца, надо ли звонящему это знать. Отпускайте только с письменным разрешением менеджера, владельца или создателя. Убедитесь, что просителя подписал договор о неразглашении тайн. Только менеджеры могут сообщать что-либо людям, не работающим в фирме.

Отвечая на просьбу дать информацию



Отвечая на просьбу о совершении действия

